Connectivity

3SKey

Guide d'utilisation du portail pour les entreprises

Ce document décrit les fonctions du portail 3SKey.

06 mars 2015

Table des matières

Préambule 3

1 Présentation du portail de clé de signature sécurisée SWIFT (3SKey) 4

1.1 Qu'est-ce que 3SKey? 4
1.2 Fonctions du portail 3SKey 6
1.3 Groupes d'utilisateurs 3SKey 8
1.4 Introduction de 3SKey dans votre organisation 11

2 Connexion 13

3 Créer un groupe d'utilisateurs (pour les administrateurs) 16

4 Ajouter un utilisateur à un groupe d'utilisateurs (pour les administrateurs) 18

5 Gérer un groupe d'utilisateurs (pour les administrateurs) 21

6 Gérer votre adresse e-mail (pour les administrateurs) 25

7 Activer un token 27

8 Renouveler un token 35

9 Configurer un token en vue d'une réinitialisation (pour les administrateurs) 43

10 Réinitialiser un token 59

11 Révoquer un token 63

12 Configurer un token en vue d'une régénération (pour les administrateurs) 67

13 Régénérer un token 70

14 Mot de passe 76

14.1 Règles en matière de mot de passe 76
14.2 Comment modifier le mot de passe 76

15 Générer le code de sécurité 78

16 Informations portées par la clé - détails du certificat et du token 79

17 Glossaire 81

18 Conditions générales 85

19 Assistance 3SKey 86

Mentions légales 89

Préambule

À propos de ce manuel

Ce document décrit les fonctions du portail 3SKey.

Modifications importantes

Le tableau suivant répertorie les changements significatifs apportés au *Guide d'utilisation du portail 3SKey pour les entreprises* depuis l'édition d'août 2013. Ce tableau ne comprend pas les différentes modifications qui ont été apportées.

Nouvelles informations	Emplacement
Clarifications apportées à la procédure de réinitialisation du token. De même, si vous utilisez une ancienne version du logiciel 3SKey, un token verrouillé peut apparaître non verrouillé durant la réinitialisation.	"Configurer un token en vue d'une réinitialisation (pour les administrateurs)", page 43
Le token ne peut pas être réinitialisé s'il se trouve en période de renouvellement. Il doit être régénéré sur un nouveau token.	"Configurer un token en vue d'une réinitialisation (pour les administrateurs)", page 43

Informations associées

Guide d'installation du token 3SKey

Mise en route de 3SKey pour les entreprises

Guide de dépannage 3SKey

1 Présentation du portail de clé de signature sécurisée SWIFT (3SKey)

1.1 Qu'est-ce que 3SKey?

Présentation

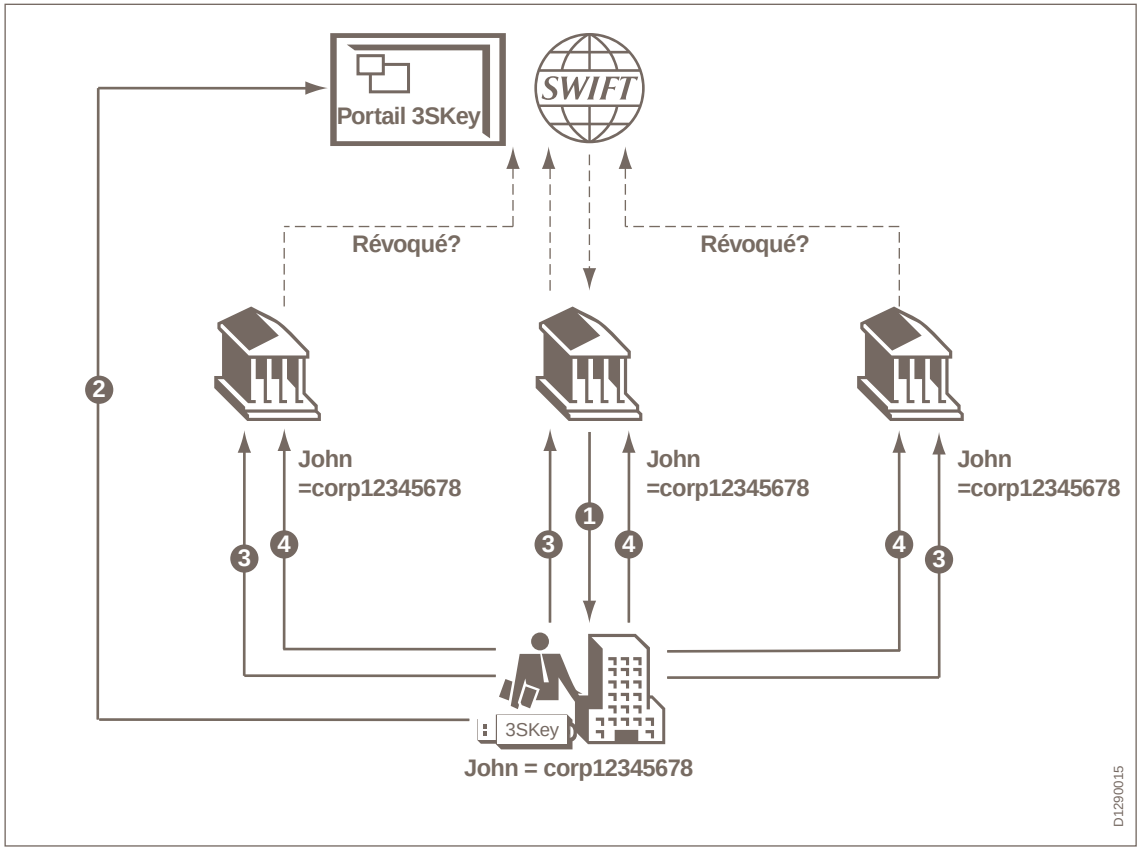
Le service 3SKey fournit un mécanisme permettant aux clients d'une banque d'authentifier et de signer les messages et les fichiers qu'ils envoient à la banque par l'intermédiaire de réseaux de services bancaires électroniques.

Lorsqu'une banque et une entreprise conviennent d'utiliser 3SKey pour authentifier les transactions, la banque fournit un ensemble de tokens 3SKey à l'entreprise, afin que chaque utilisateur individuel au sein de l'entreprise puisse recevoir un token personnel. L'utilisateur de l'entreprise doit activer le token en utilisant le portail 3SKey, puis enregistrer le token auprès de la banque.

Lorsque l'utilisateur envoie une transaction à la banque, le token crée une signature électronique pour accompagner la transaction. La signature est basée sur l'infrastructure à clé publique (PKI) SWIFT. La signature électronique permet à la banque d'identifier la personne spécifique qui a signé la transaction en utilisant la non-répudiation et de vérifier que la transaction n'a pas été modifiée depuis sa signature.

Pour plus d'informations sur 3SKey, reportez-vous à la Description du service 3SKey.

Processus de présentation de 3SKey



Les points suivants décrivent le processus 3SKey:

1. John, l'utilisateur du token 3SKey, reçoit son token de sa banque.
2. Il active son token sur le portail 3SKey.
3. Il enregistre son token auprès des banques dont il doit signer les transactions.
4. Il peut authentifier ou signer des messages en utilisant différents réseaux, tels qu'Internet, le réseau de sa banque ou SWIFT.

Parties 3SKey

Les parties suivantes sont impliquées dans la solution 3SKey:

- **SWIFT**

  SWIFT fournit le service 3SKey, le Kit du développeur 3SKey, les tokens 3SKey ainsi que le portail 3SKey nécessaire à leur gestion.

- **L'abonné 3SKey**

  L'abonné 3SKey (généralement une banque) souscrit à et intègre le service 3SKey, et distribue les tokens 3SKey aux utilisateurs 3SKey.

- **L'utilisateur 3SKey**

  L'utilisateur 3SKey (généralement une entreprise) intègre et utilise le service 3SKey avec son abonné 3SKey (ou ses abonnés 3SKey). Les utilisateurs 3SKey obtiendront normalement les tokens 3SKey auprès de leur abonné 3SKey initial.

Principes

Les principes de la solution 3SKey sont les suivants:

- SWIFT joue le rôle d'autorité de certification et fournit les certificats aux utilisateurs finals.
- Les banques distribuent des tokens contenant des clés cryptographiques inactives.
- Les utilisateurs accèdent au portail 3SKey sur Internet pour activer le token. L'activation crée des informations d'identification métier (c'est-à-dire, un certificat et une clé privée) et les stocke sur le token.
- Au lieu de contenir l'identification classique des utilisateurs telle que le nom, le prénom ou l'adresse e-mail, les certificats contiennent une identification unique sous la forme `corp12345678`.
- Au sein de la banque, le détenteur du certificat est identifié par une procédure d'association de l'identifiant unique avec l'identité réelle du détenteur.

  La procédure peut varier d'une banque à l'autre. Elle dépend des critères de sécurité propres à la banque, ou de critères établis par les réglementations du pays dans lequel le certificat est utilisé.

- Grâce à cette configuration, l'identité de l'utilisateur n'est jamais communiquée à l'extérieur de la banque. La société SWIFT elle-même ne connaît pas l'identité des détenteurs de certificat.

1.2 Fonctions du portail 3SKey

Fonctions du portail

Le portail 3SKey est utilisé uniquement pour gérer les tokens 3SKey et leurs propriétaires. Les fonctions du portail 3SKey n'ont aucun impact sur le portail de signature.

Le portail fournit les fonctions suivantes:

1. **Gérer le groupe d'utilisateurs**

   Les pages **Gestion du groupe d'utilisateurs** sont disponibles uniquement lorsque vous vous êtes connecté avec un token ayant le rôle `admin`.

   – **Créer un groupe d'utilisateurs**

     Si le portail détecte que le token avec lequel vous vous êtes connecté n'appartient pas à un groupe d'utilisateurs, il affiche un écran d'information et vous invite à créer un groupe d'utilisateurs pour votre organisation, avec deux administrateurs.

     Pour plus d'informations sur les groupes d'utilisateurs, reportez-vous à "Groupes d'utilisateurs 3SKey", page 8.

   – **Ajouter un utilisateur**

     Vous pouvez utiliser la page **Ajouter un utilisateur** pour ajouter de nouveaux utilisateurs à votre groupe d'utilisateurs et spécifier leur rôle.

     Le groupe d'utilisateurs est un ensemble de tokens 3SKey appartenant à une organisation spécifique.

     Pour des informations complémentaires, reportez-vous à "Ajouter un utilisateur à un groupe d'utilisateurs (pour les administrateurs)", page 18.

   – **Gérer un groupe d'utilisateurs**

     Vous pouvez utiliser cette page pour afficher et modifier les utilisateurs dans votre groupe d'utilisateurs.

     Pour des informations complémentaires, reportez-vous à "Gérer un groupe d'utilisateurs (pour les administrateurs)", page 21.

   – **Gérer l'adresse e-mail**

     Vous pouvez utiliser la page **Gérer l'adresse e-mail** pour enregistrer, modifier ou supprimer votre adresse e-mail. Il s'agit d'un moyen utile pour connaître les informations opérationnelles importantes sur le service 3SKey.

     Pour des informations complémentaires, reportez-vous à "Gérer votre adresse e-mail (pour les administrateurs)", page 25.

2. **Gérer le certificat sur le token**

   Ceci comprend les fonctions suivantes:

   – **Activer un token**

     Le processus d'activation 3SKey crée un **certificat métier** sur le token. Ce certificat est utilisé pour sécuriser toutes les transactions commerciales avec les banques.

     Pour des informations complémentaires, reportez-vous à "Activer un token", page 27.

   – **Renouveler un token**

Le certificat métier sur le token 3SKey est valide 3 ans après activation. Vous pouvez utiliser l'option **Renouveler** sur le portail pour renouveler le certificat métier sur un nouveau token dans les 3 mois qui précèdent sa date d'expiration.

Pour des informations complémentaires, reportez-vous à "Renouveler un token", page 35.

– **Révoquer un token**

Si un token est perdu ou compromis ou n'est plus nécessaire, le certificat associé au token peut être révoqué. Pour cela, il existe trois moyens:

- Si vous possédez toujours le token que vous souhaitez révoquer, et qu'il a été activé, vous pouvez procéder vous-même à la révocation.
- Si vous ne disposez pas du token activé que vous souhaitez révoquer ni de son mot de passe, vous pouvez demander à un administrateur d'effectuer la révocation pour votre compte.
- Si vous avez un token non activé de réserve, vous pouvez révoquer votre token activé. Toutefois, vous devrez également présenter le code de sécurité associé au token que vous souhaitez révoquer.

  Le code de sécurité a été téléchargé dans un fichier lors de l'activation du token. Par défaut, le nom du fichier est **code.txt**.

  Pour des informations complémentaires, reportez-vous à "Révoquer un token", page 63.

Lorsque le certificat est révoqué, il est ajouté à une liste de certificats révoqués. Les banques peuvent consulter cette liste avant d'autoriser une transaction: lorsqu'elles trouvent un certificat dans la liste de révocation des certificats, elles ne considèrent plus le certificat comme un certificat de confiance.

Remarque	La politique de vérification de la liste de révocation des certificats varie selon la banque. Pour savoir à quel moment elle consulte la liste, et à quelle fréquence elle la met à jour, veuillez contacter votre banque.

– **Configurer en vue d'une régénération**

Vous pouvez utiliser la page **Configurer en vue d'une régénération** pour préparer la régénération d'un token qui a été perdu ou compromis. Cette page vous permet d'attribuer un token non activé en remplacement du token d'origine.

Pour des informations complémentaires, reportez-vous à "Configurer un token en vue d'une régénération (pour les administrateurs)", page 67.

– **Régénérer un token**

Si un token est perdu, révoqué ou endommagé, vous pouvez régénérer l'identifiant unique sur un token non activé de réserve (fourni par votre banque). En conservant le même identifiant unique, vous n'avez pas à vous enregistrer à nouveau auprès des banques avec lesquelles vous êtes en relation.

L'administrateur doit configurer le nouveau token en vue d'une régénération et le rendre au propriétaire du token de réserve qui doit l'activer. Ce processus nécessite également que vous disposiez du code de sécurité du token d'origine.

Pour des informations complémentaires, reportez-vous à "Régénérer un token", page 70.

Remarque	Si vous décidez de ne pas régénérer un certificat révoqué, SWIFT vous conseille de contacter les parties associées (banques) et de les informer qu'elles ne doivent plus considérer ce certificat spécifique comme un certificat de confiance.

- **Réinitialiser un token**

  Vous pouvez utiliser cette fonctionnalité pour réutiliser un token qui est verrouillé ou dont le mot de passe est perdu.

  Au préalable, l'administrateur doit préparer le token pour la réinitialisation. Pour des informations complémentaires, reportez-vous à "Configurer un token en vue d'une réinitialisation (pour les administrateurs)", page 43.

  Ensuite, l'utilisateur du token doit finaliser la réinitialisation. Pour des informations complémentaires, reportez-vous à "Réinitialiser un token", page 59.

3. **Autres fonctions du token**

   - **Modifier le mot de passe du token**

     Vous pouvez modifier le mot de passe protégeant le contenu du token. Le mot de passe n'expire pas, mais SWIFT recommande de le modifier tous les trois mois.

     Pour des informations complémentaires, reportez-vous à "Comment modifier le mot de passe", page 76.

   - **Générer le code de sécurité**

     Un code de sécurité est associé au token. Ce code est requis s'il est nécessaire de révoquer le certificat sur le token ou de régénérer le certificat en le transférant sur un nouveau token. Le code de sécurité ne doit pas être communiqué à des tiers.

     Vous pouvez utiliser l'option **Générer le code de sécurité** si l'ancien code a été perdu ou compromis.

     Pour des informations complémentaires, reportez-vous à "Générer le code de sécurité", page 78.

   - **Informations portées par la clé**

     La page **Informations portées par la clé** affiche des informations détaillées sur le token et le certificat qu'il contient.

     Pour des informations complémentaires, reportez-vous à "Informations portées par la clé - détails du certificat et du token".

1.3 Groupes d'utilisateurs 3SKey

Qu'est-ce qu'un groupe d'utilisateurs?

Un groupe d'utilisateurs est un ensemble de tokens 3SKey appartenant à une organisation spécifique.

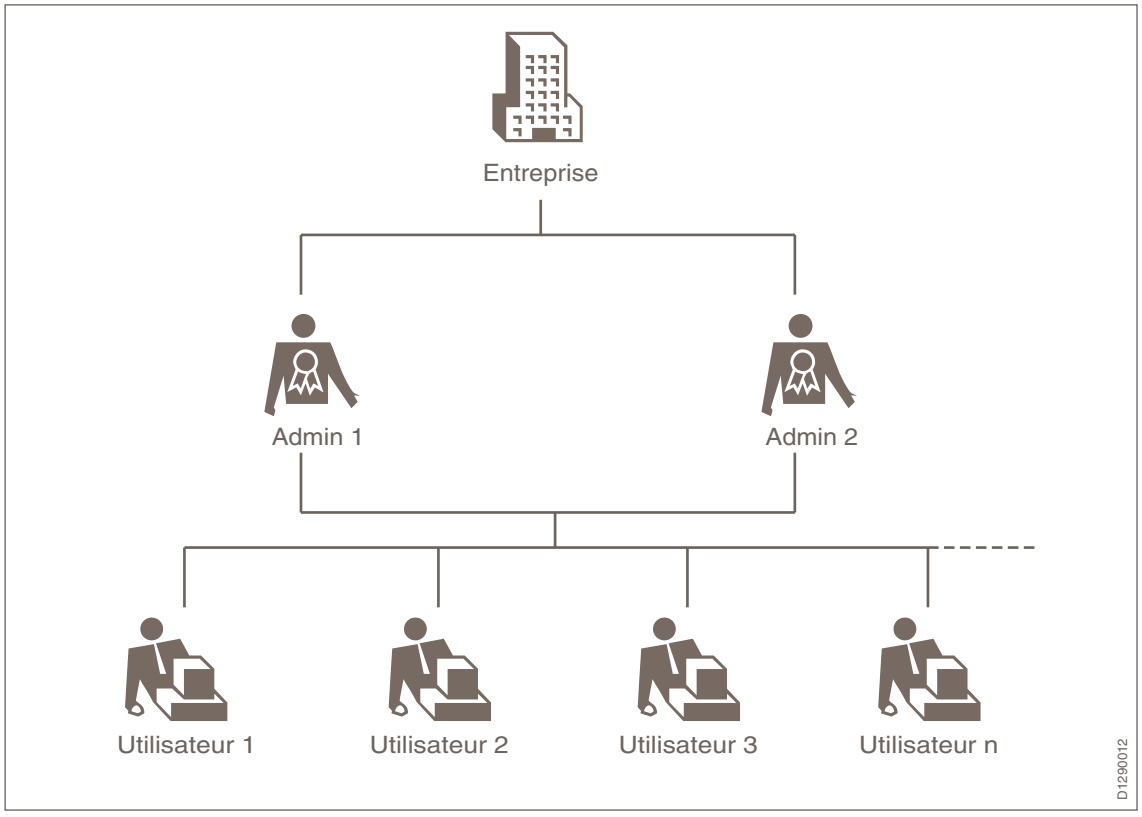
Le groupe d'utilisateurs est une aide pour gérer les tokens de l'organisation: il n'a aucun impact sur la capacité du token à signer des transactions, car l'application de signature ne connaît pas le groupe auquel le token appartient. Il est même possible de signer une transaction avec un token appartenant à un groupe, et d'approuver la transaction avec un token appartenant à un autre groupe.

La plupart des tokens dans un groupe d'utilisateurs ont le rôle `user` mais au moins deux tokens, voire plus, doivent avoir le rôle `admin`. Le rôle `admin` attribue la responsabilité de la gestion du groupe d'utilisateurs. Pour plus d'informations sur les différents types d'utilisateurs, reportez-vous à "Rôles", page 84.

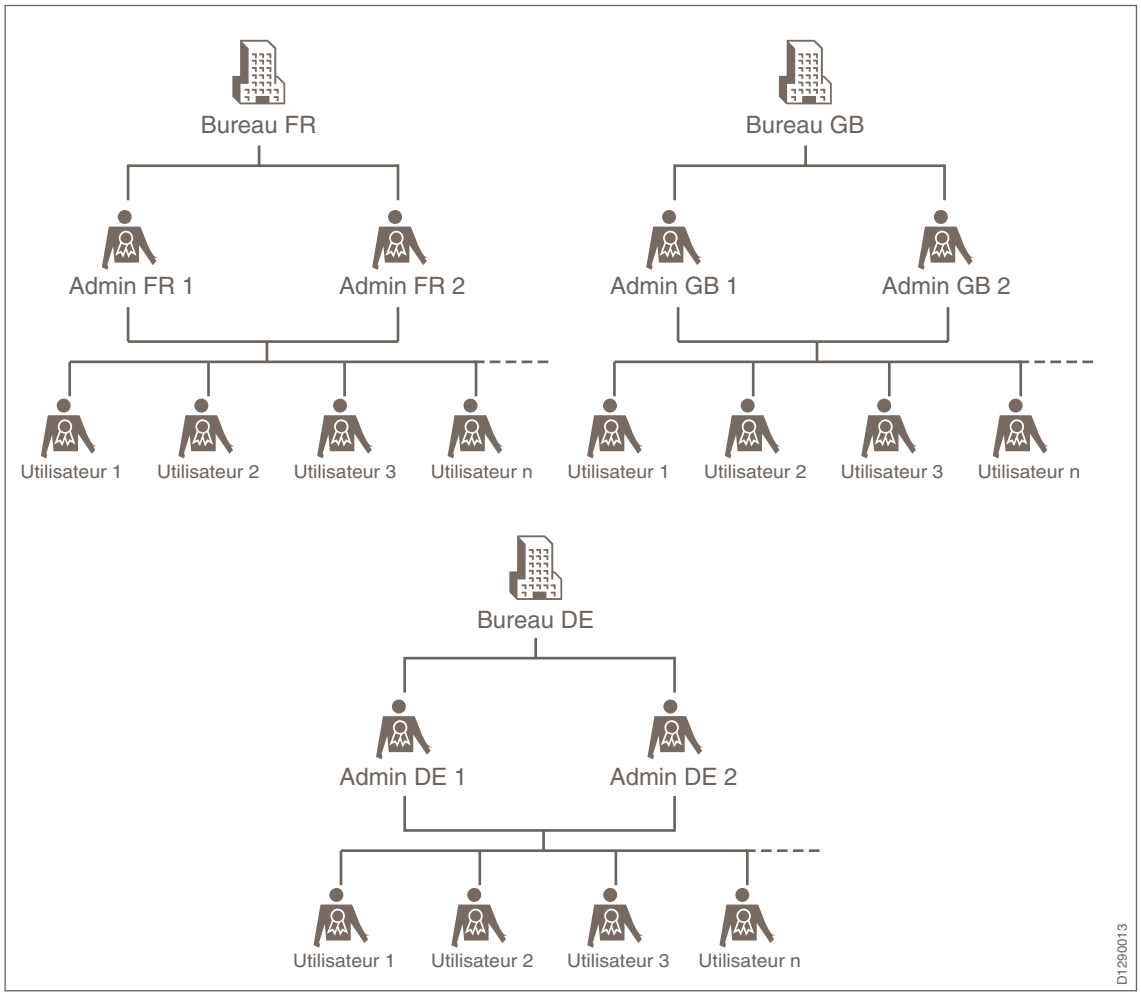
Un token utilisateur 3SKey ne peut pas être activé s'il n'appartient pas à un groupe d'utilisateurs. Un token ne peut appartenir qu'à un seul groupe d'utilisateurs.

Combien de groupes d'utilisateurs?

L'environnement 3SKey le plus simple est constitué d'un groupe d'utilisateurs unique contenant tous les tokens 3SKey appartenant à l'organisation:



Une organisation peut également avoir plusieurs groupes d'utilisateurs. Dans ce type d'environnement 3SKey, les tokens sont généralement regroupés en fonction du lieu ou du service dans lequel ils sont utilisés:



Remarque

Chaque groupe d'utilisateurs est entièrement indépendant de tous les autres groupes d'utilisateurs, y compris de ceux qui peuvent exister dans la même organisation.

Il n'est pas possible de combiner 2 groupes d'utilisateurs existants ni de diviser un groupe d'utilisateurs en 2 groupes.

Il n'y a pas de limite technique au nombre de tokens pouvant appartenir à un groupe. La principale considération pour la taille d'un groupe d'utilisateurs est l'aspect pratique. Par exemple, lorsqu'un groupe d'utilisateurs devient si important qu'il couvre plusieurs écrans sur la page **Gérer le groupe d'utilisateurs**, il devient difficile de garder une trace des tokens individuels.

Création du groupe d'utilisateurs

Lorsque vous vous connectez au portail 3SKey avec le premier token de votre organisation, il n'y a pas de groupe d'utilisateurs pour votre organisation. Le portail 3SKey détecte que votre token n'appartient à aucun groupe d'utilisateurs, et vous fait suivre le processus de création du groupe d'utilisateurs. Dans le cadre de ce processus, le portail attribue le rôle `admin` à votre token. Vous pouvez alors activer votre token, et affecter d'autres tokens au groupe d'utilisateurs.

Remarque Il doit y avoir 2 administrateurs pour la même entreprise lorsque vous commencez la création des groupes d'utilisateurs. Il est conseillé de garder quelques tokens non activés de réserve à des fins de régénération, renouvellement, ou de révocation.

Pour des informations complémentaires, reportez-vous à "Créer un groupe d'utilisateurs (pour les administrateurs)", page 16.

Si votre organisation a besoin d'un second groupe d'utilisateurs, connectez-vous au portail 3SKey avec un token que vous n'avez pas encore affecté au premier groupe d'utilisateurs. Le portail 3SKey détecte à nouveau que votre token n'appartient à aucun groupe d'utilisateurs, et vous fait suivre le processus de création du groupe d'utilisateurs.

1.4 Introduction de 3SKey dans votre organisation

Présentation

Le processus d'introduction de 3SKey dans votre organisation consiste en les étapes suivantes:

1. **Installer le logiciel du token**

   Il est nécessaire d'installer le logiciel du token sur chaque PC à partir duquel un utilisateur utilisera un token 3SKey pour accéder au portail 3SKey ou au portail de signature.

   Pour plus d'informations, reportez-vous au Guide d'installation du token 3SKey.

2. **Créer le groupe d'utilisateurs**

   Tous les tokens 3SKey doivent appartenir à un groupe d'utilisateurs.

   Lorsqu'une entreprise reçoit un lot de tokens de la part de sa banque, un administrateur configure le groupe d'utilisateurs en activant au minimum deux tokens avec des droits d'administrateur. Pour des informations complémentaires, reportez-vous à "Créer un groupe d'utilisateurs (pour les administrateurs)", page 16.

3. **Ajouter des utilisateurs**

   Une fois que les tokens administrateur ont été activés, l'administrateur ajoute des tokens non activés au groupe d'utilisateurs. Lorsqu'il est connecté au portail 3SKey, l'administrateur insère chaque token non activé à tour de rôle dans un second port USB, et l'ajoute au groupe d'utilisateurs. Pour des informations complémentaires, reportez-vous à "Ajouter un utilisateur à un groupe d'utilisateurs (pour les administrateurs)", page 18.

   Remarque Le token administrateur et le token qui est ajouté doivent être tous les deux branchés dans deux ports USB en même temps. Vous devez par conséquent ajouter les tokens au groupe d'utilisateurs avant de les distribuer à leurs propriétaires.

   Un token identifie son propriétaire comme étant un utilisateur 3SKey ou un administrateur 3SKey. Pour des informations complémentaires, reportez-vous à "Rôles", page 84.

L'administrateur répète cette opération pour tous les tokens devant être ajoutés au groupe d'utilisateurs à ce moment-là. Des tokens supplémentaires peuvent être ajoutés au groupe à tout moment.

4. **Distribuer les tokens aux utilisateurs**

   L'administrateur distribue les tokens utilisateur non activés qui appartiennent maintenant au groupe d'utilisateurs aux administrateurs ou aux utilisateurs de l'entreprise qui utiliseront les tokens.

   Le propriétaire du token a besoin des éléments suivants:

   - Le token 3SKey
   - L'identifiant unique du token (`corp99999999`). L'utilisateur doit sélectionner l'identifiant unique dans une liste déroulante lorsqu'il se connecte au portail 3SKey.
   - Le mot de passe par défaut du token
   - Les Instructions à l'attention de l'utilisateur 3SKey
   - Le Guide d'installation du token 3SKey, si le logiciel du token n'est pas déjà installé sur le PC de l'utilisateur

5. **Activer les tokens**

   Le propriétaire du token (administrateur ou utilisateur de l'entreprise) active le token en l'insérant dans un port USB sur un PC sur lequel le logiciel du token 3SKey est installé, et se connecte au portail 3SKey.

   Lorsque le propriétaire se connecte avec le token non activé et démarre l'activation, le portail 3SKey demande à l'utilisateur de remplacer le mot de passe par défaut par un mot de passe personnel.

   Le portail 3SKey génère un certificat métier sur le token, puis génère un code de sécurité personnel qui doit être conservé dans un lieu sûr par l'utilisateur.

   Le token peut alors être enregistré auprès d'une banque et être utilisé pour authentifier des transactions.

   Pour des informations complémentaires, reportez-vous à "Activer un token", page 27.

Important	Il est important d'activer les tokens avant d'envoyer les contrats d'enregistrement à la banque. Si un certificat est déjà déclaré à la banque mais que le token est perdu avant d'être activé, il est impossible de régénérer le token et le contrat doit être modifié.

2 Connexion

Présentation

Vous vous connectez au portail 3SKey en insérant votre token dans un port USB et en entrant votre mot de passe.

Conditions préalables à la connexion

Vous pouvez vérifier la configuration de votre système en effectuant un test automatique sous le menu Démarrer > **Tous les programmes** > **Swift Token Client** (Client du token SWIFT). Les résultats apparaissent après quelques secondes. Lancer le test automatique nécessite des droits d'administrateur. Si vous ne disposez pas de droits d'administrateur, veuillez vérifier chaque paramètre séparément comme indiqué ci-dessous.

Vous ne pouvez pas vous connecter au portail à moins que les conditions suivantes ne soient remplies:

- Le logiciel 3SKey est installé sur votre PC. Reportez-vous au Guide d'installation du token 3SKey pour plus d'informations.
- Une version 32 bits de l'environnement d'exécution Java (JRE) est installée sur le PC.

  Les versions minimum supportées sont:

  – 1.6.0_32 pour Java 6

  – 1.7.0_7 pour Java 7

  – 1.8.0_01 pour Java 8
- Vous pouvez vérifier votre configuration Java sur la page Java est-il installé?
- Vous devez utiliser Internet Explorer comme navigateur (la version 32 bits sur un système d'exploitation 64 bits). Les autres navigateurs ne sont pas supportés.
- Vous disposez du mot de passe du token. Le mot de passe du token est essentiel car, sans ce mot de passe, vous ne pouvez pas accéder au token.

  Si vous entrez cinq mots de passe incorrects consécutifs, le token se verrouille. Si le token se verrouille, vous devez réinitialiser le token.

La première fois que vous vous connectez avec le token, vous devez utiliser le mot de passe accompagnant le token. Si vous ne disposez pas de ce mot de passe par défaut, contactez votre administrateur 3SKey. Si la banque ayant fourni le token n'a pas envoyé le mot de passe par défaut, l'administrateur doit contacter la banque.

Commencer à se connecter

1. Insérez votre token dans un port USB.
2. Ouvrez Internet Explorer et accédez au site http:// www.3skey.com.
3. Cliquez sur Connexion.

Remarque	Dans une nouvelle session de navigateur, le portail vous invite trois fois à entrer le mot de passe du token: pour ouvrir la session SSL, pour l'authentification à Java et pour la connexion au portail 3SKey.

Connexion dans une nouvelle session de navigateur

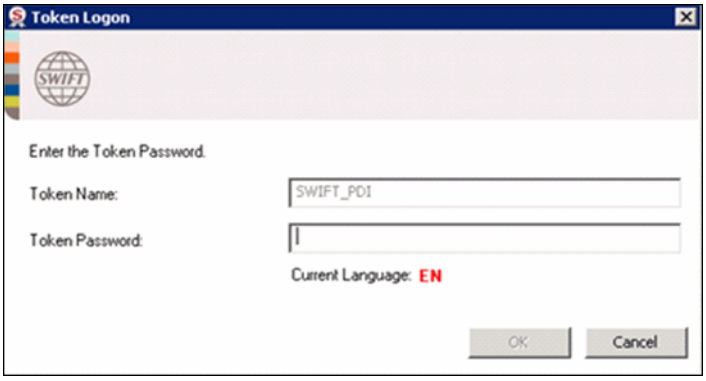
Si vous ne vous êtes pas connecté auparavant à 3SKey dans la session de navigateur actuelle, suivez la procédure ci-après:

1. Si 3SKey affiche une liste de certificats, sélectionnez l'identifiant unique du token avec lequel vous souhaitez vous connecter. L'identifiant unique se présente sous le format `corp12345678`.

   La liste contient tous les tokens actuellement connectés à votre PC, et peut également inclure les certificats personnels ayant été installés sur votre système par d'autres produits que 3SKey.

2. Cliquez sur OK.

3. Saisissez le mot de passe du token dans la fenêtre **Token Logon** (Connexion du token) et cliquez sur OK pour vous connecter au site Web sécurisé.



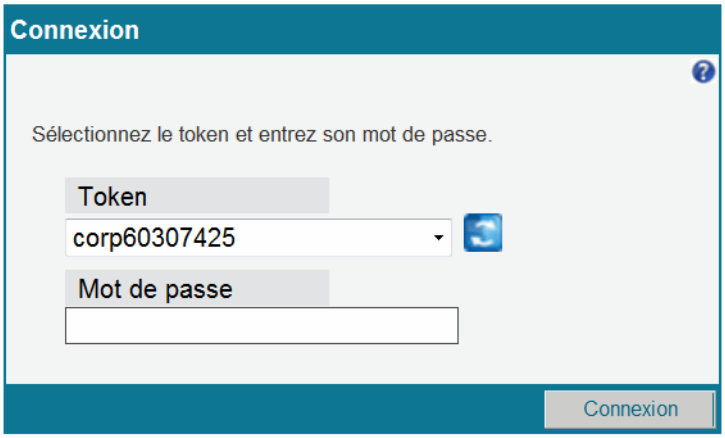
4. Si le mot de passe est accepté, l'applet Java démarre.

   Si plusieurs certificats sont installés sur votre PC, la fenêtre **Authentification requise** apparaît. Sélectionnez l'identifiant unique du token avec lequel vous souhaitez vous connecter, et cliquez sur OK.

5. Saisissez le mot de passe du token dans la fenêtre **Token Logon** (Connexion du token) et cliquez sur OK pour fournir l'authentification à Java.

Connexion au portail 3SKey

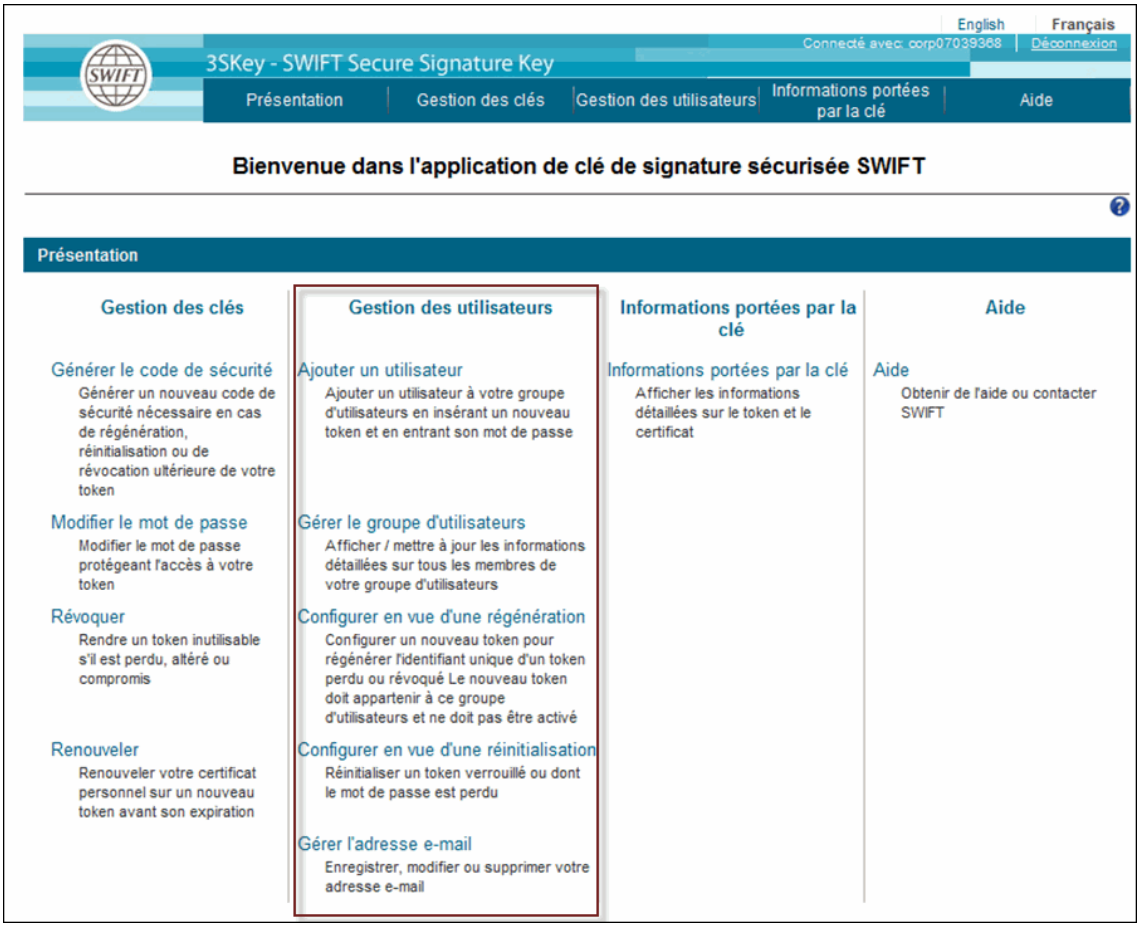
1. Sélectionnez l'identifiant unique du token dans la liste déroulante **Token** (si plusieurs tokens sont connectés au PC).



Pour afficher tous les nouveaux tokens ayant été insérés, cliquez sur Rafraîchir:

2. Saisissez le mot de passe du token et cliquez sur Connexion.

   Si vous avez le rôle `admin`, la fenêtre suivante apparaît. Si vous avez le rôle `user`, la colonne **Gestion des utilisateurs** n'apparaît pas.


English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Bienvenue dans l'application de clé de signature sécurisée SWIFT
Présentation
Gestion des clés
Générer le code de sécurité
Générer un nouveau code de sécurité nécessaire en cas de régénération, réinitialisation ou de révocation ultérieure de votre token
Modifier le mot de passe
Modifier le mot de passe protégeant l'accès à votre token
Révoquer
Rendre un token inutilisable s'il est perdu, altéré ou compromis
Renouveler
Renouveler votre certificat personnel sur un nouveau token avant son expiration
Gestion des utilisateurs
Ajouter un utilisateur
Ajouter un utilisateur à votre groupe d'utilisateurs en insérant un nouveau token et en entrant son mot de passe
Gérer le groupe d'utilisateurs
Afficher / mettre à jour les informations détaillées sur tous les membres de votre groupe d'utilisateurs
Configurer en vue d'une régénération
Configurer un nouveau token pour régénérer l'identifiant unique d'un token perdu ou révoqué Le nouveau token doit appartenir à ce groupe d'utilisateurs et ne doit pas être activé
Configurer en vue d'une réinitialisation
Réinitialiser un token verrouillé ou dont le mot de passe est perdu
Gérer l'adresse e-mail
Enregistrer, modifier ou supprimer votre adresse e-mail
Informations portées par la clé
Informations portées par la clé
Afficher les informations détaillées sur le token et le certificat
Aide
Aide
Obtenir de l'aide ou contacter SWIFT

3 Créer un groupe d'utilisateurs (pour les administrateurs)

Présentation

Si le portail détecte que le token avec lequel vous vous êtes connecté n'appartient pas à un groupe d'utilisateurs, il affiche un écran d'information et vous invite à créer un groupe d'utilisateurs pour votre organisation, avec deux administrateurs.

Pour plus d'informations sur les groupes d'utilisateurs, reportez-vous à "Groupes d'utilisateurs 3SKey", page 8.

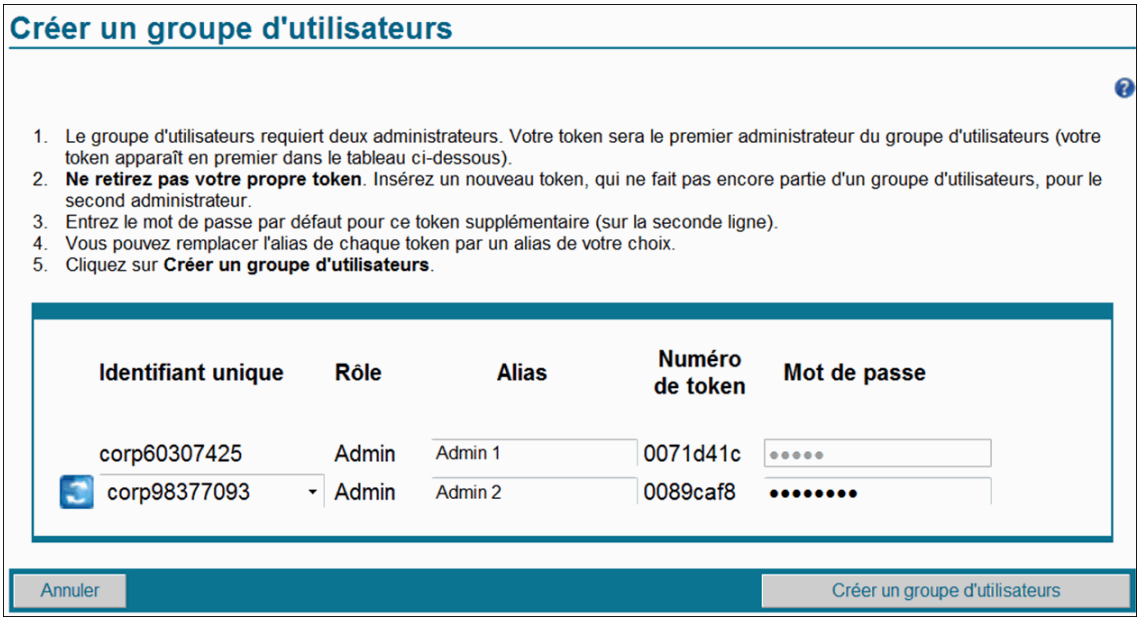
Important La création du groupe d'utilisateurs n'est pas terminée tant que vous n'avez pas créé les deux administrateurs. Vous avez par conséquent besoin de deux tokens non activés et de deux ports USB libres.

Procédure

Cette procédure suppose que vous vous êtes déjà connecté et que le système a affiché l'écran d'information qui vous invite à créer un groupe d'utilisateurs. La création du groupe d'utilisateurs consiste alors en les étapes suivantes:

1. Sur la page **Avertissement**, cliquez sur Continuer.
2. Insérez le token du second administrateur.
3. L'identifiant unique du token du second administrateur s'affiche automatiquement, précédé de l'icône .

   Le portail met à jour la page **Créer un groupe d'utilisateurs**:


Créer un groupe d'utilisateurs
1. Le groupe d'utilisateurs requiert deux administrateurs. Votre token sera le premier administrateur du groupe d'utilisateurs (votre token apparaît en premier dans le tableau ci-dessous).
2. Ne retirez pas votre propre token. Insérez un nouveau token, qui ne fait pas encore partie d'un groupe d'utilisateurs, pour le second administrateur.
3. Entrez le mot de passe par défaut pour ce token supplémentaire (sur la seconde ligne).
4. Vous pouvez remplacer l'alias de chaque token par un alias de votre choix.
5. Cliquez sur Créer un groupe d'utilisateurs.
Identifiant unique
Rôle
Alias
Numéro de token
Mot de passe
corp60307425
Admin
Admin 1
0071d41c
corp98377093
Admin
Admin 2
0089caf8
Annuler
Créer un groupe d'utilisateurs

4. Entrez le mot de passe du second token. Il s'agit du mot de passe par défaut que vous avez reçu avec les tokens.
5. Définissez un alias pour le token du second administrateur. L'alias par défaut est `Admin2`, mais vous pouvez le modifier.

6. Définissez un alias pour votre propre token. L'alias par défaut est `Admin1`, mais vous pouvez le modifier.
7. Cliquez sur Créer un groupe d'utilisateurs.

   Important Si vous laissez passer plus de cinq minutes entre les saisies, votre session risque d'arriver à expiration et de se fermer.

8. Lorsque la page **Groupe d'utilisateurs créé avec succès** s'affiche, retirez le token du second administrateur. S'il s'agit d'un token 3SKey NG-FLASH, utilisez l'icône sur la barre des tâches **Retirer le matériel en toute sécurité** .

   Transmettez le token au second administrateur, qui doit l'activer.
9. Cliquez sur Passer à l'activation pour activer votre propre token.

   Pour des informations complémentaires sur l'activation des tokens, reportez-vous à "Activer un token".

4 Ajouter un utilisateur à un groupe d'utilisateurs (pour les administrateurs)

Présentation

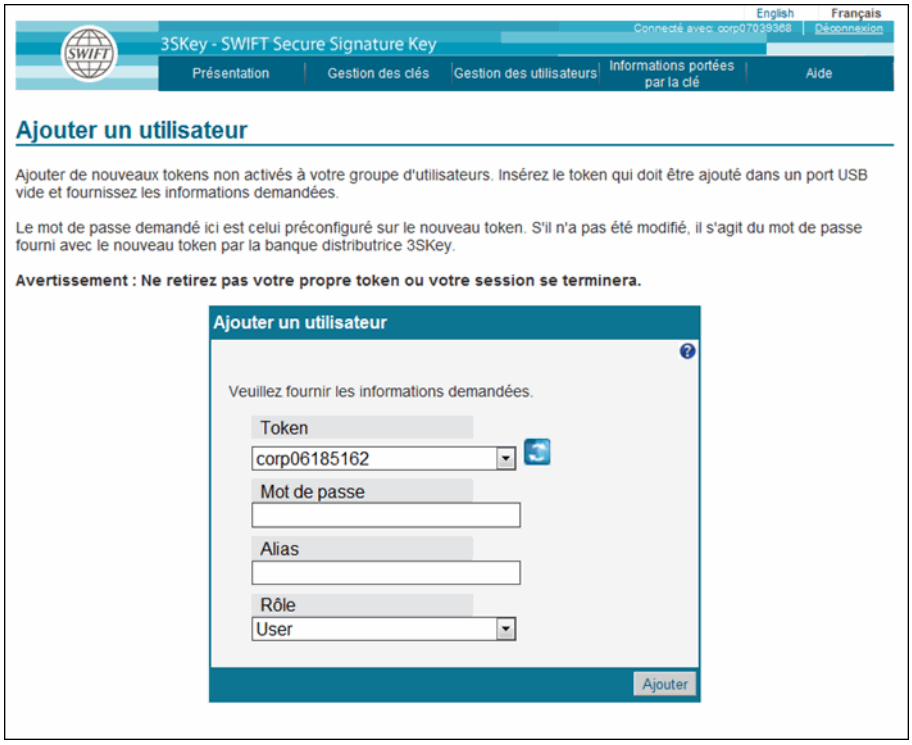
Vous pouvez utiliser cette page pour ajouter de nouveaux utilisateurs à votre groupe d'utilisateurs et spécifier leur rôle. Les utilisateurs sont identifiés par l'identifiant unique sur le token qu'ils utiliseront.

Pour chaque utilisateur que vous ajoutez, vous avez besoin d'un token `admin` et d'un nouveau token non activé. Insérez un nouveau token dans un autre port USB et renseignez les champs sur la page **Ajouter un utilisateur**.

Il est important que les deux tokens administrateur soient activés avant de commencer à ajouter des utilisateurs dans un groupe d'utilisateurs.

Important Ne retirez pas le token avec lequel vous vous êtes connecté au portail 3SKey.

Écran


English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Ajouter un utilisateur
Ajouter de nouveaux tokens non activés à votre groupe d'utilisateurs. Insérez le token qui doit être ajouté dans un port USB vide et fournissez les informations demandées.
Le mot de passe demandé ici est celui préconfiguré sur le nouveau token. S'il n'a pas été modifié, il s'agit du mot de passe fourni avec le nouveau token par la banque distributrice 3SKey.
Avertissement : Ne retirez pas votre propre token ou votre session se terminera.
Ajouter un utilisateur
Veuillez fournir les informations demandées.
Token
corp06185162
Mot de passe
Alias
Rôle
User
Ajouter

Champs

Cet écran contient les champs suivants:

Token

Sélectionnez l'identifiant unique du nouveau token dans la liste déroulante.

Si vous ne voyez pas l'identifiant unique correct, cliquez sur Rafraîchir pour actualiser la liste:

Mot de passe

Indiquez le mot de passe fourni avec le nouveau token.

Alias

Vous pouvez utiliser le champ **Alias** pour spécifier un nom avec lequel identifier l'identifiant unique, par exemple le rôle de l'utilisateur auquel il a été attribué, ou **Token de réserve**.

L'alias est utilisé uniquement au sein de votre organisation pour gérer les tokens sur le portail 3SKey. Il n'a aucune incidence sur l'utilisation du token pour signer des transactions et il n'est pas nécessaire de communiquer l'alias à la banque.

Vous pouvez utiliser les caractères suivants pour l'alias:

`A-Z`

`a-z`

`0-9`

`_ - ,` et espace

Vous ne pouvez pas utiliser de caractères accentués (é ou ö par exemple), ni de signes de ponctuation exceptés ceux qui sont répertoriés.

Rôle

Le rôle attribué à un identifiant unique détermine les fonctions auxquelles un utilisateur peut accéder lorsqu'il est connecté avec cet identifiant unique.

Par défaut, les identifiants uniques sont ajoutés au groupe d'utilisateurs avec le rôle `user`. Vous pouvez également créer un administrateur en sélectionnant `admin` dans la liste déroulante.

- Un token avec le rôle `user` donne accès aux fonctions suivantes:
  - Utiliser le certificat sur le token pour signer ou authentifier des transactions avec une banque
  - Modifier le mot de passe du token
  - Générer un nouveau code de sécurité
  - Révoquer le certificat sur le token
  - Effectuer la régénération du certificat sur le token

    Pour cela, un second token préparé par un administrateur en vue d'une régénération est nécessaire. Pour des informations complémentaires, reportez-vous à "Régénérer un token", page 70.
  - Procéder à la réinitialisation d'un token configuré en vue d'une réinitialisation par un administrateur
  - Afficher les informations portées par la clé stockées sur le token (par exemple, l'identifiant unique et la période de validité)
  - Renouveler le token avant son expiration (au bout de trois ans)
- Un token avec le rôle `admin` donne accès aux mêmes fonctions qu'un token avec le rôle `user`. Ces fonctions sont identiques pour les deux types d'utilisateurs.

  En outre, les tokens avec le rôle `admin` donnent accès aux fonctions suivantes:
  - Configurer et maintenir un groupe d'utilisateurs contenant des tokens avec le rôle `admin` et des tokens avec le rôle `user`

- Afficher les tokens et le statut des tokens dans le groupe d'utilisateurs
- Révoquer les tokens des utilisateurs dans le groupe
- Configurer un token pour la régénération d'un identifiant unique (rôle `user` ou rôle `admin`)
- Configurer en vue d'une réinitialisation un token verrouillé ou dont le mot de passe est perdu

Finaliser l'ajout du token

Lorsque tous les champs sont renseignés correctement, cliquez sur Ajouter.

Le portail 3SKey confirme que le token a été ajouté au groupe d'utilisateurs.

Ajouter un utilisateur
L'identifiant unique corp60919434 a été attribué à votre User groupe le 10 juillet 2012 15:54:31 CEST
Ajouter un autre
Effectué

Retirez le token que vous avez ajouté du port USB. S'il s'agit d'un token 3SKey NG-FLASH, utilisez l'icône sur la barre des tâches **Retirer le matériel en toute sécurité** .

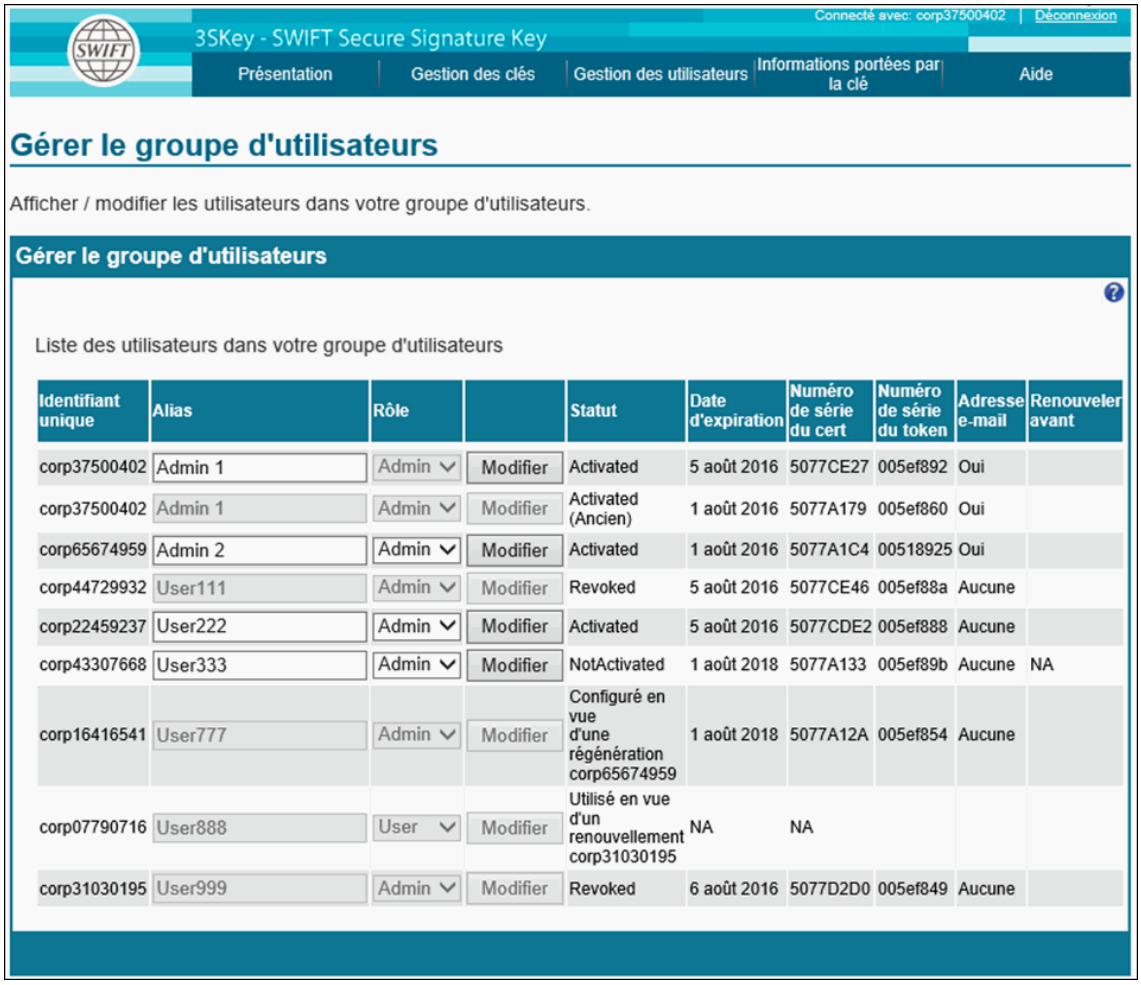
- Si d'autres tokens doivent être ajoutés au groupe d'utilisateurs, cliquez sur Ajouter un autre.
- Si vous avez fini d'ajouter tous les tokens au groupe d'utilisateurs, cliquez sur Effectué.

5 Gérer un groupe d'utilisateurs (pour les administrateurs)

Présentation

Vous pouvez utiliser cette page pour afficher les utilisateurs dans votre groupe d'utilisateurs, et pour modifier leurs rôles et alias. Cette page est disponible uniquement lorsque vous vous êtes connecté avec un token ayant le rôle `admin`.

Écran


Connecté avec: corp37500402 | Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Gérer le groupe d'utilisateurs
Afficher / modifier les utilisateurs dans votre groupe d'utilisateurs.
Gérer le groupe d'utilisateurs
Liste des utilisateurs dans votre groupe d'utilisateurs
Identifiant unique | Alias | Rôle | | Statut | Date d'expiration | Numéro de série du cert | Numéro de série du token | Adresse e-mail | Renouveler avant
corp37500402 | Admin 1 | Admin | Modifier | Activated | 5 août 2016 | 5077CE27 | 005ef892 | Oui
corp37500402 | Admin 1 | Admin | Modifier | Activated (Ancien) | 1 août 2016 | 5077A179 | 005ef860 | Oui
corp65674959 | Admin 2 | Admin | Modifier | Activated | 1 août 2016 | 5077A1C4 | 00518925 | Oui
corp44729932 | User111 | Admin | Modifier | Revoked | 5 août 2016 | 5077CE46 | 005ef88a | Aucune
corp22459237 | User222 | Admin | Modifier | Activated | 5 août 2016 | 5077CDE2 | 005ef888 | Aucune
corp43307668 | User333 | Admin | Modifier | NotActivated | 1 août 2018 | 5077A133 | 005ef89b | Aucune | NA
corp16416541 | User777 | Admin | Modifier | Configuré en vue d'une régénération corp65674959 | 1 août 2018 | 5077A12A | 005ef854 | Aucune
corp07790716 | User888 | User | Modifier | Utilisé en vue d'un renouvellement corp31030195 | NA | NA
corp31030195 | User999 | Admin | Modifier | Revoked | 6 août 2016 | 5077D2D0 | 005ef849 | Aucune

Champs

Le groupe d'utilisateurs contient les champs suivants:

Identifiant unique

Identifiant unique du token.

Alias

Nom défini par l'utilisateur pour identifier l'identifiant unique. L'alias est utilisé uniquement au sein de votre organisation pour gérer les tokens sur le portail 3SKey.

Vous pouvez utiliser les caractères suivants pour l'alias:

`A-Z`

`a-z`

`0-9`

`_ - ,` et espace

Vous ne pouvez pas utiliser de caractères accentués (é ou ö par exemple), ni de signes de ponctuation exceptés ceux qui sont répertoriés.

Rôle

Utilisez la liste déroulante pour attribuer à l'utilisateur le rôle `user` ou le rôle `admin`.

- Les utilisateurs avec le rôle `user` ont accès aux fonctions suivantes:
  - Utiliser le certificat sur le token pour signer ou authentifier des transactions avec une banque
  - Modifier le mot de passe du token
  - Générer un nouveau code de sécurité
  - Révoquer le certificat sur le token
  - Effectuer la régénération du certificat sur le token. Pour cela, un second token préparé par un administrateur en vue d'une régénération est nécessaire
  - Procéder à la réinitialisation d'un token configuré en vue d'une réinitialisation par un administrateur
  - Afficher les informations portées par la clé stockées sur le token (par exemple, l'identifiant unique et la période de validité)
  - Renouveler le token avant son expiration (au bout de trois ans)
- Les utilisateurs avec le rôle `admin` ont accès à toutes les fonctions du rôle `user`, plus les fonctions suivantes:
  - Configurer et maintenir un groupe d'utilisateurs contenant des tokens avec le rôle `admin` et des tokens avec le rôle `user`
  - Afficher les tokens et le statut des tokens dans le groupe d'utilisateurs
  - Révoquer les tokens des utilisateurs dans le groupe
  - Configurer un token pour la régénération d'un identifiant unique (rôle `user` ou rôle `admin`)
  - Réinitialiser un token **Non activé**
  - Configurer en vue d'une réinitialisation un token **Activé** qui est verrouillé ou dont le mot de passe est perdu

Mettre à jour le groupe d'utilisateurs

Lorsque vous avez spécifié **l'alias** et **le rôle**, cliquez sur Modifier pour enregistrer vos modifications. Vous devez effectuer cette opération pour chaque **identifiant unique** pour lequel des changements ont été apportés aux champs **Alias** et **Rôle**.

Statut

Statut actuel du token. Ce champ peut contenir les valeurs suivantes:

Activated (Activé)	Le token a été activé comme token d'utilisateur ou d'administrateur.
Activated (old) (Activé (ancien))	Ce token a été renouvelé mais est toujours valide.
NotActivated (Non activé))	Le token est toujours à l'état d'origine, non activé. Lorsque le statut du certificat est **NotActivated** (Non activé), vous pouvez: • Activer le token pour une utilisation normale. Pour des informations complémentaires, reportez-vous à "Activer un token", page 27. • Configurer le token pour régénérer un autre token qui est inutilisable. Pour des informations complémentaires, reportez-vous à "Régénérer un token", page 70. • Utiliser le token pour révoquer un autre token. Pour des informations complémentaires, reportez-vous à "Méthode 3: Utiliser un token non activé pour révoquer un token", page 65. • Utiliser le token pour renouveler un token sur le point d'expirer. Pour des informations complémentaires, reportez-vous à "Renouveler un token", page 35.
NotActivated (Reset Interrupted) (Non activé (réinitialisation interrompue))	La procédure de réinitialisation a été interrompue pour une raison quelconque (par exemple, une coupure de réseau). Il est nécessaire de redémarrer la procédure de réinitialisation.
Prepared to recover (corp12345678) (Préparé en vue d'une régénération (corp12345678))	Le token a été configuré pour régénérer un autre token qui est inutilisable. La régénération n'a pas encore été effectuée.
Prepared to reset (corp12345678) (Préparé en vue d'une réinitialisation (corp12345678))	Le token a été configuré par l'administrateur et est prêt à être réinitialisé par l'utilisateur.
Revoked (Révoqué)	Le token a été révoqué et ne peut plus être utilisé. Ce statut s'applique uniquement aux tokens révoqués par une action de **révocation** explicite, il ne s'applique pas aux tokens révoqués dans le cadre du processus de **régénération**.
Used to recover (corp12345678) (Utilisé pour la régénération (corp12345678))	Le token a été utilisé pour régénérer un autre token qui est inutilisable. L'identifiant unique qui était associé à l'origine au token converti n'est plus actif. La liste des utilisateurs contient une seconde entrée avec le même numéro de token mais un identifiant unique différent, avec le statut **Activated** (Activé). L'identifiant unique est celui du token qui a été régénéré.

Used to renew (corp12345678) (Utilisé pour le renouvellement (corp12345678))	Cela signifie que le token contenant le certificat repris sous la colonne **Identifiant unique** a été utilisé pour renouveler un token. L'identifiant unique du nouveau certificat qui en résulte apparaît dans la colonne **Statut**. Par exemple, dans l'écran ci-dessus, l'identifiant unique (corp07790716) était initialement présent sur le token (numéro de série 005EF849). Ce token a été utilisé pour renouveler corp31030195. Après renouvellement, le token portant le numéro de série 005EF849 a un nouveau certificat avec l'identifiant unique corp31030195. L'identifiant unique d'origine (corp07790716) n'est plus utilisé.

Date d'expiration

Date et heure d'expiration du certificat.

Numéro de série du certificat

Numéro de série du certificat.

Numéro de série du token

Numéro de série imprimé sur le token.

Adresse e-mail

Indique si un utilisateur avec le rôle `admin` a enregistré une adresse e-mail pour le service:

- **Oui**: une adresse e-mail a été enregistrée.
- **Aucune**: aucune adresse e-mail n'a été enregistrée.

Renouveler avant

Nombre de jours avant que le certificat ne doive être renouvelé.

6 Gérer votre adresse e-mail (pour les administrateurs)

Présentation

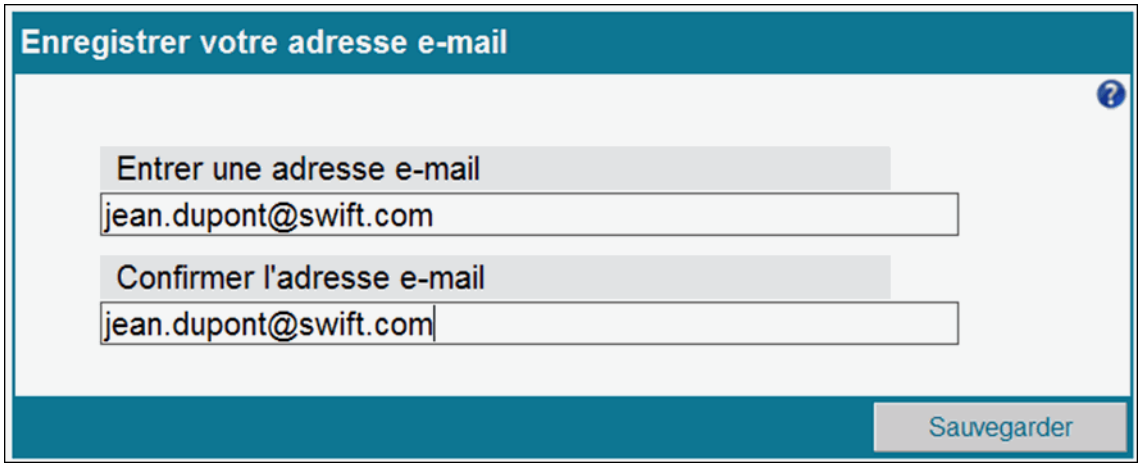
Vous pouvez utiliser cette page pour enregistrer, modifier ou supprimer votre adresse e-mail. Cette page est disponible uniquement lorsque vous vous êtes connecté avec un token ayant le rôle `admin`.

SWIFT recommande vivement aux administrateurs 3SKey d'enregistrer une adresse e-mail, afin de pouvoir recevoir les notifications opérationnelles concernant le service 3SKey.

SWIFT utilise cette adresse e-mail uniquement pour communiquer des informations opérationnelles importantes sur le service 3SKey, telles qu'une mise à niveau obligatoire de logiciel, une modification apportée aux fonctions, ou une modification des conditions générales que vous devez connaître.

Pour des informations sur la protection des données et la manière dont SWIFT traite vos données personnelles, reportez-vous à la section *"Protection des données personnelles"* dans les Conditions générales de 3SKey. Seule fait foi la dernière version en anglais disponible sur www.swift.com > À propos de SWIFT > Informations légales > Contrats SWIFT.

Écran



Champs

Entrer une adresse e-mail

Entrez l'adresse e-mail que vous souhaitez que SWIFT utilise pour les notifications opérationnelles.

Confirmer l'adresse e-mail

Confirmez votre adresse e-mail en la saisissant de nouveau.

Rapport de certificats arrivant à expiration

Si vous avez enregistré votre adresse e-mail, vous recevrez régulièrement le **rapport de certificats arrivant à expiration**.

Ce rapport contient une liste de tous les certificats au sein de votre groupe d'utilisateurs qui arrivent à expiration dans les 90 jours.

UID	Token serial number	Expiration date
corp14829882	01dd9762	8/1/2016 14:31
corp21580981	01dd971a	8/1/2016 14:39

Ce rapport est uniquement envoyé s'il y a au moins un token qui arrive à expiration dans votre groupe d'utilisateurs et sera renvoyé toutes les 3 semaines. Vous recevrez par e-mail un rapport similaire à celui qui suit. Dans le rapport, le format de date d'expiration est le suivant `mm/jj/aaaa`. Dans l'exemple ci-dessus, les tokens expirent le 1er août 2016.

Cher Administrateur 3SKey,

Certains tokens 3SKey dans votre groupe d'utilisateurs arrivent à expiration (vous en trouverez la liste en pièce jointe).
Avant que ces tokens ne deviennent inutilisables, leurs utilisateurs doivent renouveler leurs certificats sur de nouveaux tokens 3SKey.
Nous vous invitons à contacter la banque qui vous a fourni ces tokens 3SKey pour en commander de nouveaux.

Le processus de renouvellement est décrit sur le site 3SKey sous http://www.swift.com/3skey/fr/renewal.html

Remarque Si vous ne souhaitez plus recevoir de notifications concernant un token expiré que vous ne souhaitez pas régénérer, vous devez le révoquer.

7 Activer un token

Contexte

Lorsque vous recevez votre token de la banque, il contient un **certificat technique** qui est valide durant 5 ans. Vous devez activer le token avant que le **certificat technique** n'expire. Cela signifie que vous avez 5 ans pour activer le token.

Pour préparer votre token pour pouvoir l'utiliser, vous devez **activer** le token. Le processus d'activation crée un **certificat métier** sur le token. Ce certificat est utilisé pour sécuriser toutes les transactions commerciales avec la banque et est valide durant 3 ans.

Le token peut être utilisé sur d'autres ordinateurs sur lesquels le logiciel d'installation du token 3SKey est installé.

Il est essentiel d'activer le token **avant** de communiquer les identifiants uniques à votre banque. Si vous enregistrez un token non activé et que vous ne parvenez pas à l'activer (car vous l'avez perdu ou endommagé), il est nécessaire de modifier tout contrat associé que vous avez déjà envoyé à votre banque. Il est impossible de régénérer l'identifiant unique d'un token non activé.

Remarque	Si vous avez le rôle `admin`, vous ne pouvez pas accéder aux fonctions d'administrateur sur le portail 3SKey tant que vous n'avez pas activé le token.

Important	Vous ne pouvez pas activer un token s'il n'appartient pas à un groupe d'utilisateurs.

Présentation de la procédure

Une fois que vous vous êtes connecté avec un token inactif, une page vous permettant de démarrer le processus d'activation s'ouvre. L'activation du token consiste en les étapes suivantes:

1. Initialiser le processus d'activation en cliquant sur Suivant.
2. Modifier le mot de passe qui protège le token.

   Vous utilisez ce mot de passe pour vous connecter au portail 3SKey et pour signer vos transactions.
3. Enregistrer une adresse e-mail.

   Cette étape est facultative, uniquement pour les administrateurs 3SKey.
4. Le portail génère le certificat métier et le stocke sur le token.
5. Le portail génère le code de sécurité que vous devez télécharger et conserver dans un lieu sûr.

Démarrer l'activation

Pour procéder à l'activation, cliquez sur Suivant.

Remarque Lors de l'activation de votre token, vous pouvez ignorer le message sur la page **Activation du token** indiquant "pour utiliser ce token à des fins de révocation uniquement, annulez cette étape...". Ceci s'applique uniquement si vous utilisez un token non activé pour rendre un autre token inutilisable s'il a été perdu ou compromis, ou si le propriétaire a quitté l'organisation. Reportez-vous à la section "Méthode 3: Utiliser un token non activé pour révoquer un token", page 65 pour plus d'informations.

Si vous cliquez sur Annuler par erreur, vous pouvez reprendre l'activation en cliquant sur **Activer**.

Important

- **Ne fermez pas le navigateur et ne retirez pas le token du logement USB.**

  Le token risquerait d'être altéré. Si une autre tentative d'activation du token échoue, vous devez alors utiliser un nouveau token.

- **Le délai d'activation expire au bout de cinq minutes.**

  Lorsqu'une opération requiert que vous fournissiez deux informations différentes, vous devez fournir la seconde information dans les cinq minutes suivant la première. Sinon, votre session peut arriver à expiration et vous devez recommencer le processus d'activation.

Modifier le mot de passe par défaut

1. Lorsque vous cliquez sur Suivant sur la page **Activation du token**, la page **Modifier le mot de passe du token** apparaît.

English
Français
3SKey - SWIFT Secure Signature Key
Étapes de l'activation
1. Modifier le mot de passe
2. Enregistrer une adresse e-mail
3. Générer la clé
4. Code de sécurité
5. Terminé
Modifier le mot de passe du token
Vous devez modifier le mot de passe initial du token.
Assurez-vous de vous souvenir du nouveau mot de passe. Sans ce mot de passe, vous ne serez pas en mesure d'accéder au token..
Modifier le mot de passe du token
Sélectionnez un nouveau mot de passe pour votre token.
Les règles pour les mots de passe sont les suivantes:
• La longueur minimale est de quatre caractères.
• Caractères autorisés 0..9 A..Z a..z !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ et espace.
• Vous devez utiliser au moins deux caractères différents.
• Vous ne pouvez pas réutiliser la valeur actuelle ou précédente du mot de passe.
Mot de passe actuel
Nouveau mot de passe
Confirmation du nouveau mot de passe
Modifier

Entrez le mot de passe initial fourni avec le token dans le champ **Mot de passe actuel**.

Fournissez un mot de passe sécurisé. Suivez les directives ci-après lorsque vous créez un mot de passe:

- La longueur minimale est de quatre caractères
- La longueur maximale est de seize caractères
- Vous pouvez utiliser les caractères suivants:

  – `0-9 A-Z a-z` et espace

  `_ ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~`

- Vous devez utiliser au moins deux caractères différents. Par exemple, vous ne pouvez pas définir le mot de passe sur `aaaa` ou `11111`
- Vous ne pouvez pas utiliser de caractères accentués (é ou ö par exemple)
- Vous ne pouvez pas réutiliser le mot de passe actuel ni le mot de passe précédent

2. Cliquez sur Modifier.

   La page **Modifier le mot de passe du token** apparaît avec le texte `Le mot de passe a été modifié avec succès`.

English
Français
3SKey - SWIFT Secure Signature Key
Étapes de l'activation
Modifier le mot de passe du token
1. Modifier le mot de passe
Assurez-vous de vous souvenir du nouveau mot de passe. Sans ce mot de passe, vous ne serez pas en mesure d'accéder au token..
2. Enregistrer une adresse e-mail
Modifier le mot de passe du token
Le mot de passe a été modifié avec succès
Suivant
3. Générer la clé
4. Code de sécurité
5. Terminé

Important	Assurez-vous de conserver votre mot de passe dans un endroit sûr.

Remarque	Il n'y a pas de date d'expiration associée au mot de passe.

3. Cliquez sur Suivant.

Enregistrer une adresse (pour les administrateurs)

La page **Enregistrer une adresse e-mail** apparaît uniquement lors de l'activation d'un token auquel le rôle `admin` est affecté.

English
Français
3SKey - SWIFT Secure Signature Key
Étapes de l'activation
1. Modifier le mot de passe
2. Enregistrer une adresse e-mail
3. Générer la clé
4. Code de sécurité
5. Terminé
Enregistrer une adresse e-mail
Veuillez spécifier une adresse e-mail que SWIFT peut utiliser pour vous avertir des mises à jour opérationnelles importantes concernant le service 3SKey.
Enregistrer votre adresse e-mail
Entrer une adresse e-mail
Confirmer l'adresse e-mail
Sauvegarder
SWIFT traitera vos données personnelles conformément à la section "Personal Data Protection" des 3SKey Terms & Conditions sur www.swift.com > À propos de SWIFT > Aspect légal > Contrats SWIFT.

SWIFT recommande vivement aux administrateurs 3SKey d'enregistrer une adresse e-mail pour le service, afin de pouvoir recevoir les notifications opérationnelles concernant le service 3SKey.

SWIFT utilisera cette adresse e-mail uniquement pour communiquer des informations opérationnelles importantes sur le service 3SKey, telles qu'une mise à niveau obligatoire de logiciel, une modification apportée aux fonctions, ou une modification des conditions générales que vous devez connaître.

Pour des informations sur la protection des données et la manière dont SWIFT traite vos données personnelles, reportez-vous à la section Protection des données personnelles dans les Conditions générales de 3SKey. Seule fait foi la dernière version en anglais disponible sur www.swift.com > À propos de SWIFT > Informations légales >Contrats SWIFT.

L'enregistrement et la gestion de votre adresse e-mail sont entièrement sous votre contrôle. Sur le portail 3SKey, vous pouvez enregistrer, modifier ou supprimer votre adresse e-mail à tout moment.

1. **Entrer une adresse e-mail**

   Entrez l'adresse e-mail que vous souhaitez que SWIFT utilise pour les notifications opérationnelles.

2. **Confirmer l'adresse e-mail**

   Confirmez votre adresse e-mail en la saisissant de nouveau.

3. Cliquez sur Enregistrer.

Générer la clé

Le portail affiche la page **Générer la clé** pour afficher sa progression lors des étapes suivantes:

- Générer la demande d'activation
- Obtenir le certificat auprès de SWIFT
- Enregistrer le nouveau certificat sur le token

- Confirmer l'activation du token à SWIFT

English
Français
3SKey - SWIFT Secure Signature Key
Étapes de l'activation
1. Modifier le mot de passe
2. Enregistrer une adresse e-mail
3. Générer la clé
4. Code de sécurité
5. Terminé
Générer la clé
Votre token est en cours d'activation. Vous recevrez un code de sécurité. Veuillez enregistrer le fichier et noter ce code pour référence ultérieure.
Ne retirez pas votre token pendant l'activation.
Générer la clé et demander la certification
Obtenir le certificat auprès de SWIFT
Enregistrer le nouveau certificat sur le token
Confirmer l'activation du token à SWIFT

Si l'étape **Générer la clé** a été effectuée avec succès, cela signifie que le nouveau certificat métier a été généré et certifié.

Important L'activation de la clé peut prendre quelques secondes. N'annulez pas l'opération en fermant le navigateur ou en déconnectant le token. Le token pourrait devenir inutilisable.

Si le portail ne répond plus pendant plus de 5 minutes (en raison d'un problème de réseau), vous devez redémarrer le navigateur et ré-essayer l'opération. Vous devrez vous connecter en utilisant le nouveau mot de passe.

Générer le code de sécurité

Le portail génère ensuite le code de sécurité:

1. Cliquez sur Télécharger pour enregistrer le code de sécurité dans un fichier.

   Le portail vous invite à enregistrer le fichier, avec le nom **code.txt** dans le dossier par défaut de votre navigateur. Le cas échéant, vous pouvez modifier le nom du fichier et le dossier.

2. Cliquez sur Confirmer une fois le téléchargement terminé.

3. Vérifiez si le fichier téléchargé contient un code de 16 caractères (quatre groupes de quatre caractères, séparés par des tirets).

   Important Vous devez conserver le code de sécurité dans un endroit sûr. S'il est nécessaire de régénérer ou de réinitialiser le token, ceci est impossible sans le code de sécurité.

   Ne stockez pas le code de sécurité sur le token 3SKey NG-FLASH lui-même, ou avec votre token.

   Si vous stockez le code de sécurité sur votre PC et que vous changez de PC, n'oubliez pas de supprimer le code de sécurité de l'ancien PC et stockez-le sur le nouveau.

Remarque Si vous avez perdu le code de sécurité, vous pouvez vous connecter au portail 3SKey et générer un nouveau code pour autant que votre token fonctionne toujours. Si votre token ne fonctionne pas (s'il est verrouillé, expiré ou révoqué), vous aurez besoin de votre code de sécurité parce que vous ne pouvez pas en générer un nouveau avec un token qui ne fonctionne pas.

Pour plus d'informations sur comment générer le code de sécurité, reportez-vous à "Générer le code de sécurité", page 78.

Activation effectuée

La fenêtre **Activation effectuée** apparaît.

English
Français
Connecté avec: corp46141684
Déconnexion
3SKey - SWIFT Secure Signature Key
Étapes de l'activation
1. Modifier le mot de passe
2. Enregistrer une adresse e-mail
3. Générer la clé
4. Code de sécurité
5. Terminé
Activation effectuée
Le processus d'activation a été effectué avec succès.
Une fois que vous aurez enregistré votre clé auprès de votre banque, vous pourrez signer les messages adressés à votre banque. Assurez-vous de connaître votre identifiant de clé et votre code de sécurité. Votre identifiant de clé est affiché dans le coin supérieur droit de l'écran.
Important: Maintenant, déconnectez-vous, retirez puis réinsérez le token activé.

Votre token est à présent activé, et vous pouvez l'enregistrer auprès de votre banque. Vous pouvez alors l'utiliser pour authentifier et signer des transactions commerciales.

Vous pouvez utiliser le token sur n'importe quel PC sur lequel le logiciel du token 3SKey est installé.

Remarque Lorsque vous insérez le token, vous ajoutez les informations sur le certificat du token dans le magasin de certificats du navigateur sur le PC que vous utilisez.

Si vous souhaitez utiliser le token immédiatement sur le PC que vous avez utilisé pour l'activation, vous devez ajouter les informations sur le certificat les plus récentes au magasin de certificats. Déconnectez-vous du portail 3SKey et retirez le token du port USB. S'il s'agit d'un token 3SKey NG-FLASH, utilisez l'icône sur la barre des tâches **Retirer le matériel en toute sécurité** . Réinsérez ensuite le token dans le port USB.

Que faire en cas de problème avec l'activation

Si le processus d'activation échoue pour une raison quelconque, effectuez les opérations suivantes:

1. Fermez votre navigateur Internet Explorer.
2. Ouvrez une session Internet Explorer et accédez au site http:// www.3skey.com.
3. Connectez-vous.

   Remarque Si vous avez modifié votre mot de passe pendant la tentative précédente d'activation du token, vous devez utiliser le nouveau mot de passe pour vous connecter.

4. Recommencez le processus d'activation. Le processus commence au point où il s'était arrêté auparavant.

Lorsqu'un token est activé, il est utilisé pour signer des transactions. Un token 3SKey activé n'est pas limité au système sur lequel il a été activé, il peut également signer des transactions sur différents systèmes.

8 Renouveler un token

Présentation

Les tokens 3SKey comprennent un certificat métier qui reste valide 3 ans à partir de la date d'activation du token. Par exemple, un token activé le 1er janvier 2011 comprend un certificat qui expire le 1er janvier 2014.

SWIFT recommande aux utilisateurs de renouveler les certificats sur un nouveau token au moins 2 mois avant la date d'expiration du certificat.

Avertissement Il est important de renouveler un certificat à temps. Si le certificat expire, il ne peut plus être utilisé pour signer des transactions ni accéder au portail 3SKey et doit être régénéré.

Les administrateurs 3SKey peuvent enregistrer une adresse e-mail afin de recevoir les détails des certificats arrivant à expiration. Pour plus d'informations, reportez-vous à la section "Gérer votre adresse e-mail (pour les administrateurs)", page 25.

Conditions préalables au renouvellement du token

Avant qu'un utilisateur ne puisse renouveler le certificat métier contenu sur le token, les conditions suivantes doivent être remplies:

- Le certificat à renouveler doit se trouver dans sa période de renouvellement (c'est-à-dire dans les 3 mois avant son expiration).
- L'utilisateur doit avoir reçu un nouveau token et un mot de passe par défaut de son administrateur.
- Le PC utilisé pour le renouvellement doit disposer de 2 ports USB libres.

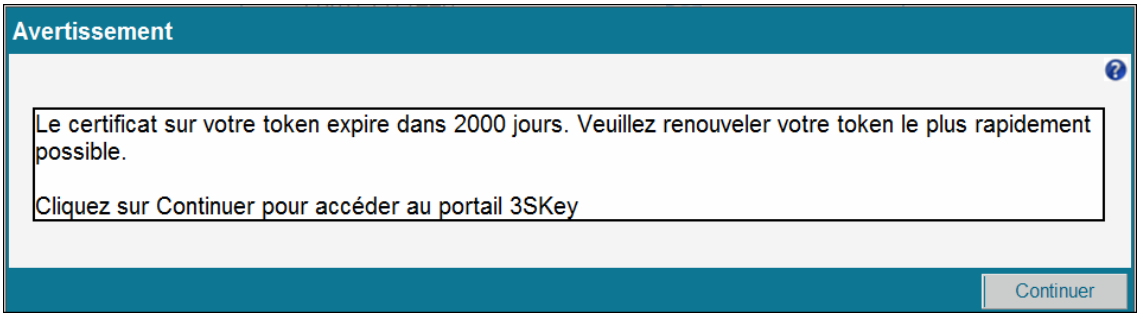
Remarque Il n'est pas nécessaire d'ajouter le nouveau token à un groupe d'utilisateurs avant la procédure de renouvellement.

Procédure de renouvellement du token

Lorsque les conditions préalables sont remplies, l'utilisateur du token peut renouveler son certificat comme suit:

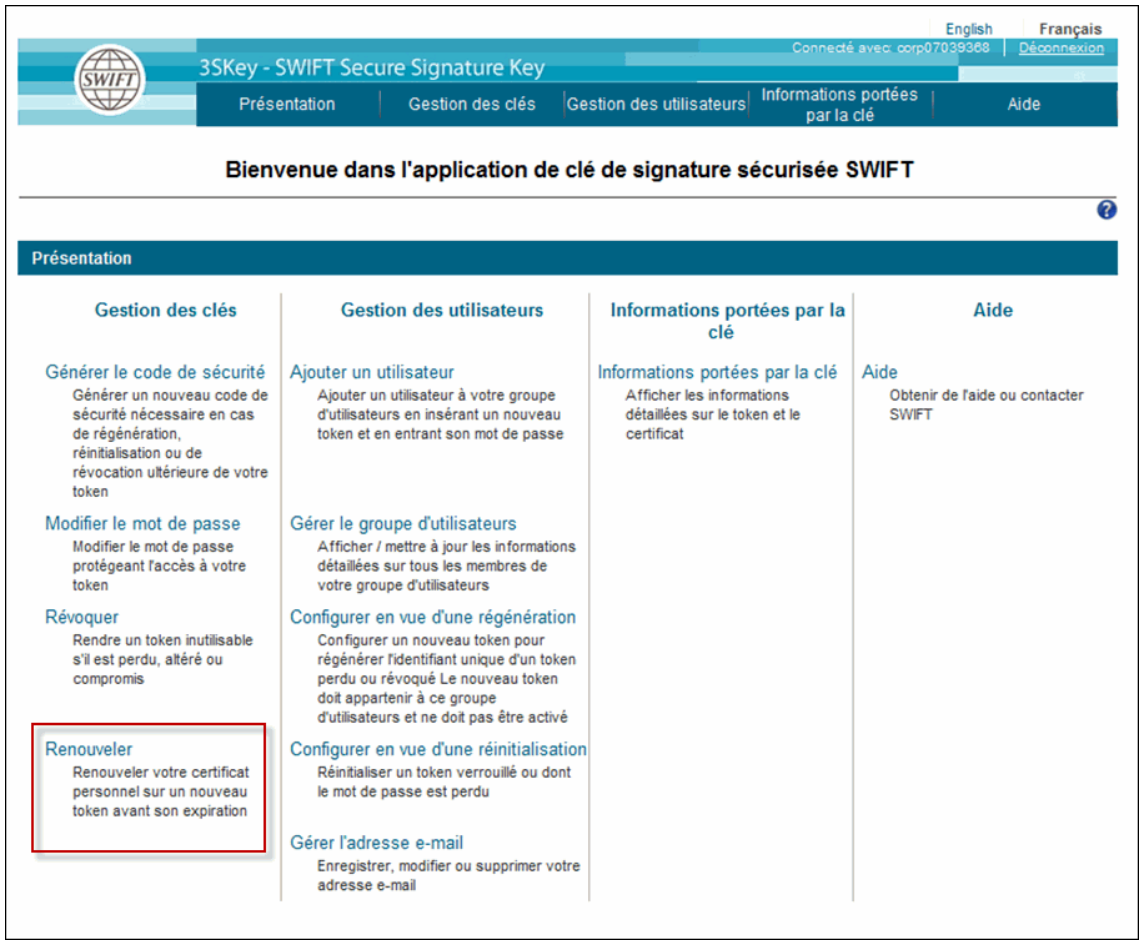
1. Insérez votre token actuel dans un port USB de votre PC et accédez à 3SKey.com, cliquez sur Connexion et saisissez le mot de passe de votre token actuel.

   La fenêtre suivante apparaît.


Avertissement
Le certificat sur votre token expire dans 2000 jours. Veuillez renouveler votre token le plus rapidement possible.
Cliquez sur Continuer pour accéder au portail 3SKey
Continuer

   Cliquez sur Continuer.

2. La fenêtre **Présentation** s'affiche automatiquement. Notez que la colonne **Gestion des utilisateurs** ne s'affiche que si vous avez le rôle `admin`.


English
Français
Connecté avec corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Bienvenue dans l'application de clé de signature sécurisée SWIFT
Présentation
Gestion des clés
Générer le code de sécurité
Générer un nouveau code de sécurité nécessaire en cas de régénération, réinitialisation ou de révocation ultérieure de votre token
Modifier le mot de passe
Modifier le mot de passe protégeant l'accès à votre token
Révoquer
Rendre un token inutilisable s'il est perdu, altéré ou compromis
Renouveler
Renouveler votre certificat personnel sur un nouveau token avant son expiration
Gestion des utilisateurs
Ajouter un utilisateur
Ajouter un utilisateur à votre groupe d'utilisateurs en insérant un nouveau token et en entrant son mot de passe
Gérer le groupe d'utilisateurs
Afficher / mettre à jour les informations détaillées sur tous les membres de votre groupe d'utilisateurs
Configurer en vue d'une régénération
Configurer un nouveau token pour régénérer l'identifiant unique d'un token perdu ou révoqué Le nouveau token doit appartenir à ce groupe d'utilisateurs et ne doit pas être activé
Configurer en vue d'une réinitialisation
Réinitialiser un token verrouillé ou dont le mot de passe est perdu
Gérer l'adresse e-mail
Enregistrer, modifier ou supprimer votre adresse e-mail
Informations portées par la clé
Informations portées par la clé
Afficher les informations détaillées sur le token et le certificat
Aide
Aide
Obtenir de l'aide ou contacter SWIFT

Cliquez sur **Renouveler** dans la colonne **Gestion des clés**.

3. Si le token doit être renouvelé, la fenêtre **Renouvellement du token** apparaît.

Connecté avec: corp15311448 | Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes du renouvellement
1. Démarrer le renouvellement
2. Sélectionner le nouveau token
3. Modifier le mot de passe
4. Générer la clé
5. Terminé
Renouveler
Renouvellement du token
Le certificat sur votre token expire le 1 août 2016 11:30:24 CEST et doit être renouvelé sur un nouveau token.
Ce processus peut prendre quelques minutes et ne peut pas être interrompu. Ne fermez pas votre navigateur et ne retirez aucun des tokens jusqu'à ce que le processus soit terminé.
Sans retirer votre token, veuillez insérer un nouveau token non activé et cliquer sur Suivant.
Annuler
Suivant

Insérez le nouveau token dans le PC sans retirer le token actuel et cliquez sur Suivant.

Avertissement Ne retirez aucun des deux tokens durant le processus de renouvellement.

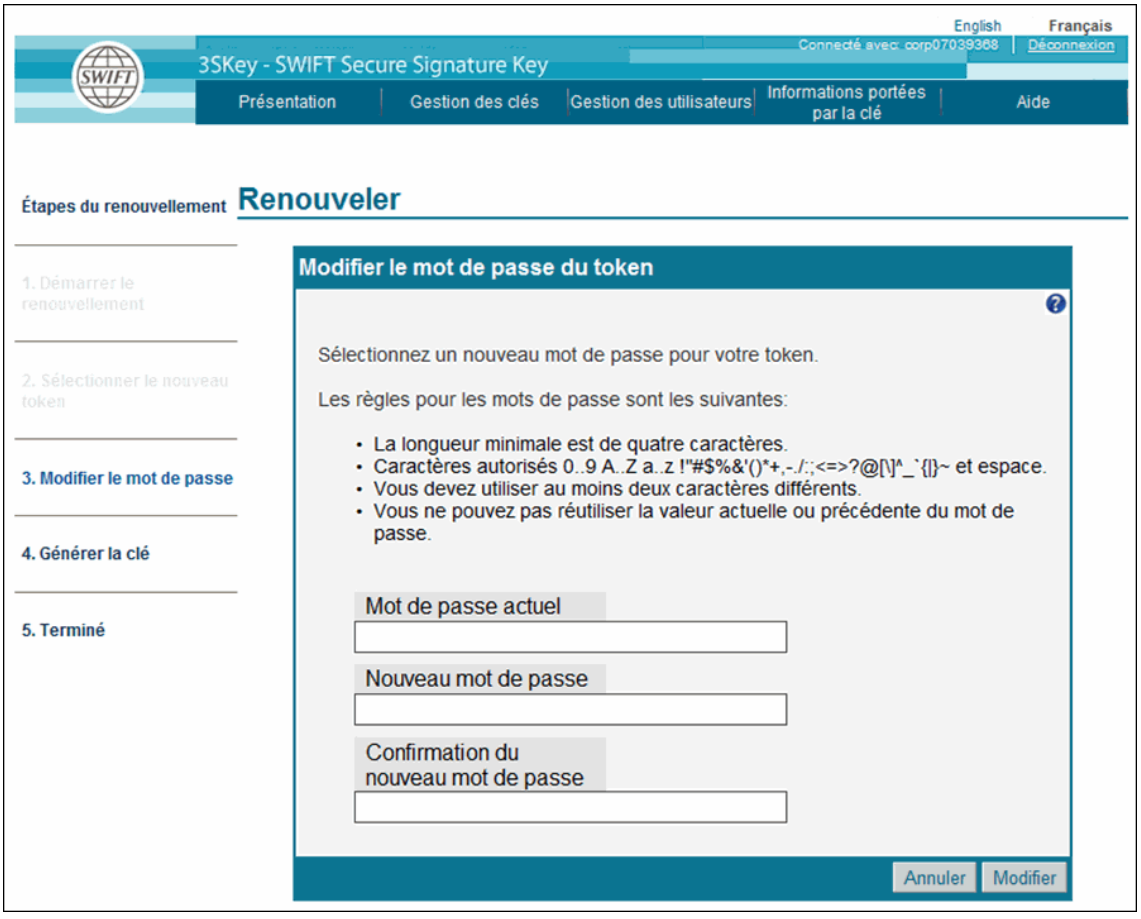
4. La fenêtre **Sélectionner le nouveau token** apparaît.

Connecté avec: corp15311448 | Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes du renouvellement
1. Démarrer le renouvellement
2. Sélectionner le nouveau token
3. Modifier le mot de passe
4. Générer la clé
5. Terminé
Renouveler
Sélectionner le nouveau token
Sélectionnez un nouveau token et entrez son mot de passe.
Le mot de passe demandé ici est celui préconfiguré sur le nouveau token. S'il n'a pas été modifié, il s'agit du mot de passe fourni avec le nouveau token par la banque distributrice 3SKey.
Numéro de série du token
01dd976d
Mot de passe
Annuler
Suivant

Dans la liste déroulante à droite du champ **Numéro de série du token**, sélectionnez le numéro de série de votre nouveau token (disponible sur le token même).

Introduisez le mot de passe par défaut que vous avez reçu de votre banque ou de votre administrateur et cliquez sur Suivant.

5. La fenêtre **Modifier le mot de passe du token** apparaît.


English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes du renouvellement
Renouveler
1. Démarrer le renouvellement
2. Sélectionner le nouveau token
3. Modifier le mot de passe
4. Générer la clé
5. Terminé
Modifier le mot de passe du token
Sélectionnez un nouveau mot de passe pour votre token.
Les règles pour les mots de passe sont les suivantes:
• La longueur minimale est de quatre caractères.
• Caractères autorisés 0..9 A..Z a..z !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ et espace.
• Vous devez utiliser au moins deux caractères différents.
• Vous ne pouvez pas réutiliser la valeur actuelle ou précédente du mot de passe.
Mot de passe actuel
Nouveau mot de passe
Confirmation du nouveau mot de passe
Annuler
Modifier

Introduisez le mot de passe par défaut du nouveau token dans le champ **Mot de passe actuel**.

Introduisez un nouveau mot de passe, conforme aux règles qui apparaissent à l'écran et ré-introduisez le nouveau mot de passe.

Cliquez sur Modifier.

Remarque Gardez votre mot de passe en sécurité. Si vous perdez le mot de passe ou que vous entrez 5 mots de passe incorrects consécutifs, le token se verrouille et il est nécessaire de le réinitialiser.

Le nouveau mot de passe est défini pour le nouveau token uniquement. Le mot de passe de l'ancien token reste inchangé.

6. Un message confirmant que la modification du mot de passe a réussi s'affiche.

Cliquez sur Suivant.

7. Le processus de renouvellement du certificat se lance automatiquement.

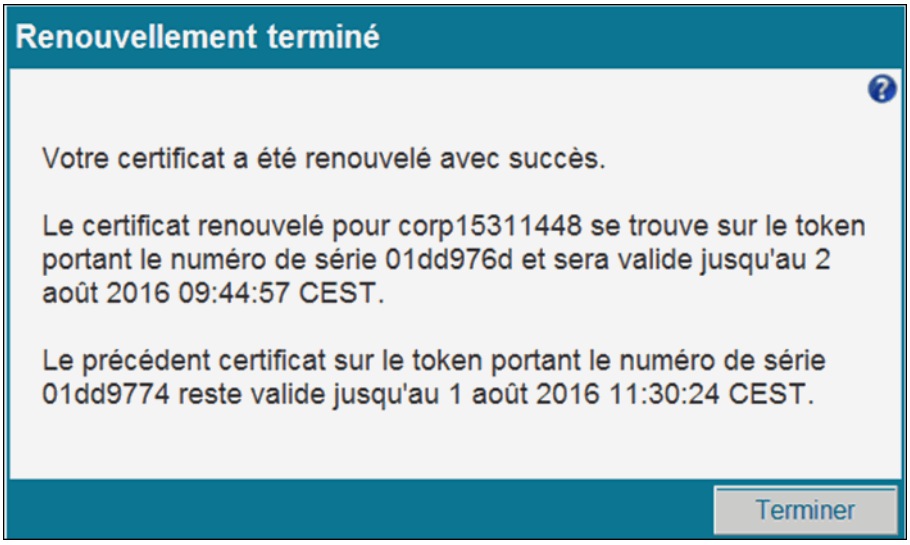
Connecté avec: corp15311448 | Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes du renouvellement
1. Démarrer le renouvellement
2. Sélectionner le nouveau token
3. Modifier le mot de passe
4. Générer la clé
5. Terminé
Renouveler
Votre certificat est en cours de renouvellement sur le nouveau token.
Avertissement: ne retirez pas vos tokens pendant le renouvellement.
Générer la clé et demander la certification
Obtenir le certificat auprès de SWIFT
Enregistrer le nouveau certificat sur le token
Confirmer le renouvellement du token à SWIFT

Lorsque le processus de renouvellement est terminé, la fenêtre **Renouvellement terminé** apparaît.

Important Le renouvellement de la clé peut prendre quelques secondes. N'annulez pas l'opération en fermant le navigateur ou en déconnectant le token. Le token pourrait devenir inutilisable.

Si le portail ne répond plus pendant plus de 5 minutes (en raison d'un problème de réseau), vous devez redémarrer le navigateur et ré-essayer l'opération. Veuillez noter que le mot de passe sur le nouveau token sera celui que vous avez modifié. Vous devrez saisir ce mot de passe dans la fenêtre **Sélectionner le nouveau token** (voir étape 4) et le modifier à nouveau dans la fenêtre **Modifier le mot de passe du token** (voir étape 5).

8.


Renouvellement terminé
Votre certificat a été renouvelé avec succès.
Le certificat renouvelé pour corp15311448 se trouve sur le token portant le numéro de série 01dd976d et sera valide jusqu'au 2 août 2016 09:44:57 CEST.
Le précédent certificat sur le token portant le numéro de série 01dd9774 reste valide jusqu'au 1 août 2016 11:30:24 CEST.
Terminer

Cliquez sur Terminer.

Le certificat métier a été renouvelé sur le nouveau token (et activé avec le même identifiant unique) et est prêt à être utilisé.

Remarque Une fois le renouvellement terminé, SWIFT recommande de vous déconnecter immédiatement du portail et de retirer les tokens du PC. Vous pouvez vous connecter à la prochaine session 3SKey en utilisant le nouveau token.

Essayer de renouveler un token qui a déjà été renouvelé

Le certificat sur le token ne peut être renouvelé que tous les 3 ans. Si vous vous connectez avec un token qui se trouve en période d'expiration et qui a été renouvelé et que vous cliquez sur le menu **Renouveler**, une fenêtre vous confirmant que le renouvellement n'est pas nécessaire s'ouvre.

Renouvellement du token
Votre certificat pour corp97807019 a déjà été renouvelé sur le token portant le numéro de série 00123456789
Annuler

Comme c'est le cas avec n'importe quel autre token, si le nouveau token est perdu ou verrouillé, il doit être régénéré ou réinitialisé en utilisant l'identifiant unique et le code de sécurité.

Si vous accédez au portail avec un ancien token qui a été renouvelé, les seules fonctionnalités disponibles sont les suivantes **Modifier le mot de passe**, **Révoquer** et **Informations portées par la clé**.

Connecté avec: corp15311448 | Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Informations portées par la clé
Aide
Bienvenue dans l'application de clé de signature sécurisée SWIFT
Présentation
Gestion des clés
Modifier le mot de passe
Modifier le mot de passe protégeant l'accès à votre token
Révoquer
Rendre un token inutilisable s'il est perdu, altéré ou compromis
Informations portées par la clé
Informations portées par la clé
Afficher les informations détaillées sur le token et le certificat
Aide
Aide
Obtenir de l'aide ou contacter SWIFT

Essayer de renouveler un token qui se trouve en dehors de la période d'expiration

Si vous cliquez sur le menu **Renouveler** en étant connecté avec un token qui n'a pas besoin d'être renouvelé, la fenêtre suivante s'affiche et vous explique quand vous pouvez renouveler le certificat.

English
Français
Connecté avec: corp07039368 | Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes du renouvellement
Renouveler
1. Démarrer le renouvellement
2. Sélectionner le nouveau token
3. Modifier le mot de passe
4. Générer la clé
5. Terminé
Renouvellement du token
Votre certificat ne peut pas encore être renouvelé. Veuillez réessayer après le 7 novembre 2016 12:22:13 EST.
Votre certificat (corp07039368) expire le 5 février 2017 12:22:13 EST.
Annuler

Renouvellement terminé

Suite au processus de renouvellement, vous disposez de 2 tokens. Un ancien token (renouvelé) contenant l'ancien certificat (toujours valide) et un nouveau token contenant un nouveau certificat valide pour une durée de 3 ans. Jusqu'à ce que l'ancien token expire, les 2 tokens apparaissent dans la fenêtre **Gestion des utilisateurs** (fonctionnalité uniquement disponible pour les administrateurs d'entreprise).

Durant la période où vous disposerez de 2 tokens, SWIFT vous recommande de différencier le nouveau token de l'ancien token (en utilisant un porte-clés ou un autocollant par exemple) pour éviter toute confusion.

Afin de vérifier si vous utilisez un ancien token (non expiré) ou un token contenant un certificat renouvelé, connectez-vous avec le token que vous souhaitez vérifier et consultez la date d'émission (champ **Émis**) sur la page **Informations portées par la clé**.

Consultez les instructions de votre banque afin de savoir si votre nouveau certificat doit être enregistré auprès de la banque et la procédure requise, si nécessaire.

- Si vous ne devez pas enregistrer votre nouveau token auprès de votre banque, SWIFT vous recommande de commencer à utiliser votre nouveau token même si l'ancien token est encore valide.
- Si votre banque requiert que le nouveau token soit enregistré, veuillez procéder à l'enregistrement immédiatement afin d'être en mesure d'utiliser le nouveau token le plus rapidement possible. Votre ancien token peut toujours être utilisé temporairement.

Lorsque toutes vos banques ont enregistré le nouveau token, SWIFT recommande d'utiliser uniquement le nouveau certificat sur le nouveau token.

Vous ne pouvez vous séparer de l'ancien token qu'après expiration de son certificat. Séparez-vous de l'ancien token de la même manière que vous le feriez pour n'importe quel autre outil électronique au sein de votre organisation.

Remarque Le code de sécurité du token d'origine reste valide. Si vous souhaitez remplacer le code de sécurité, reportez-vous à "Générer le code de sécurité", page 78.

9 Configurer un token en vue d'une réinitialisation (pour les administrateurs)

Présentation

Vous devez procéder à la réinitialisation du token lorsque vous devez:

- Réinitialiser un token verrouillé ou dont le mot de passe est perdu. La réinitialisation ne s'applique qu'aux tokens dont le statut est:
  - **Activated** (Activé)
  - **Activated (Reset Interrupted)** (Activé (réinitialisation interrompue))
  - **NotActivated** (Non activé))
  - **NotActivated (Reset Interrupted)** (Non activé (réinitialisation interrompue))
  - **Prepared to recover** (Préparé en vue d'une régénération)
  - **Prepared to reset** (Préparé en vue d'une réinitialisation)
- Retirer un token **non activé** de son groupe d'utilisateurs
- Faire passer le statut d'un token de **Prepared to recover** (Préparé en vue d'une régénération) à **Not activated** (Non activé) et le retirer de son groupe d'utilisateurs

Vous devez remplir les conditions préalables suivantes pour réinitialiser un token:

- Vous devez disposer du rôle `admin`.
- Vous devez vous assurer que deux ports USB libres sont disponibles sur le PC sur lequel vous souhaitez procéder à la réinitialisation.
- Pour réinitialiser un token activé, l'utilisateur du token doit disposer de son code de sécurité.

Important Si vous ne disposez pas de votre code de sécurité, vous ne pouvez pas réinitialiser le token et vous devez activer un nouveau token avec un identifiant unique différent. Un token qui a été configuré en vue d'une réinitialisation dont le code de sécurité a été perdu est inutilisable.

Le code de sécurité a été téléchargé dans un fichier lors de l'activation du token. Par défaut, le nom du fichier est **code.txt** et il est stocké dans le dossier par défaut de votre navigateur.

Remarque Le nombre maximum de réinitialisations par token est de 5. Si un token se verrouille ou devient inutilisable après 5 réinitialisations, un nouveau token est nécessaire.

Pourquoi ne puis-je pas réinitialiser un token?

Vous ne pouvez pas réinitialiser un token expiré, révoqué ou qui se verrouille durant sa période de renouvellement (c'est-à-dire 90 jours avant son expiration). Vous devrez régénérer son identifiant unique sur un nouveau token. Consultez l'écran ci-dessous comme exemple.

Réinitialiser le token
Sélectionner le token
04221: Le certificat sur le token à réinitialiser se trouve en période de renouvellement. Vous pouvez utiliser la fonction de régénération pour le régénérer sur un nouveau token.
Sélectionner le token à réinitialiser:
0070c5e1
Annuler
Suivant

Pour régénérer un token, reportez-vous à "Configurer un token en vue d'une régénération (pour les administrateurs)", page 67.

Comment réinitialiser un token

1. Connectez-vous au portail 3SKey en utilisant votre token `admin`.
2. Cliquez sur **Configurer en vue d'une ré-initialisation** sur la page **Présentation**.

English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Bienvenue dans l'application de clé de signature sécurisée SWIFT
Présentation
Gestion des clés
Générer le code de sécurité
Générer un nouveau code de sécurité nécessaire en cas de régénération, réinitialisation ou de révocation ultérieure de votre token
Modifier le mot de passe
Modifier le mot de passe protégeant l'accès à votre token
Révoquer
Rendre un token inutilisable s'il est perdu, altéré ou compromis
Renouveler
Renouveler votre certificat personnel sur un nouveau token avant son expiration
Gestion des utilisateurs
Ajouter un utilisateur
Ajouter un utilisateur à votre groupe d'utilisateurs en insérant un nouveau token et en entrant son mot de passe
Gérer le groupe d'utilisateurs
Afficher / mettre à jour les informations détaillées sur tous les membres de votre groupe d'utilisateurs
Configurer en vue d'une régénération
Configurer un nouveau token pour régénérer l'identifiant unique d'un token perdu ou révoqué Le nouveau token doit appartenir à ce groupe d'utilisateurs et ne doit pas être activé
Configurer en vue d'une réinitialisation
Réinitialiser un token verrouillé ou dont le mot de passe est perdu
Gérer l'adresse e-mail
Enregistrer, modifier ou supprimer votre adresse e-mail
Informations portées par la clé
Informations portées par la clé
Afficher les informations détaillées sur le token et le certificat
Aide
Aide
Obtenir de l'aide ou contacter SWIFT

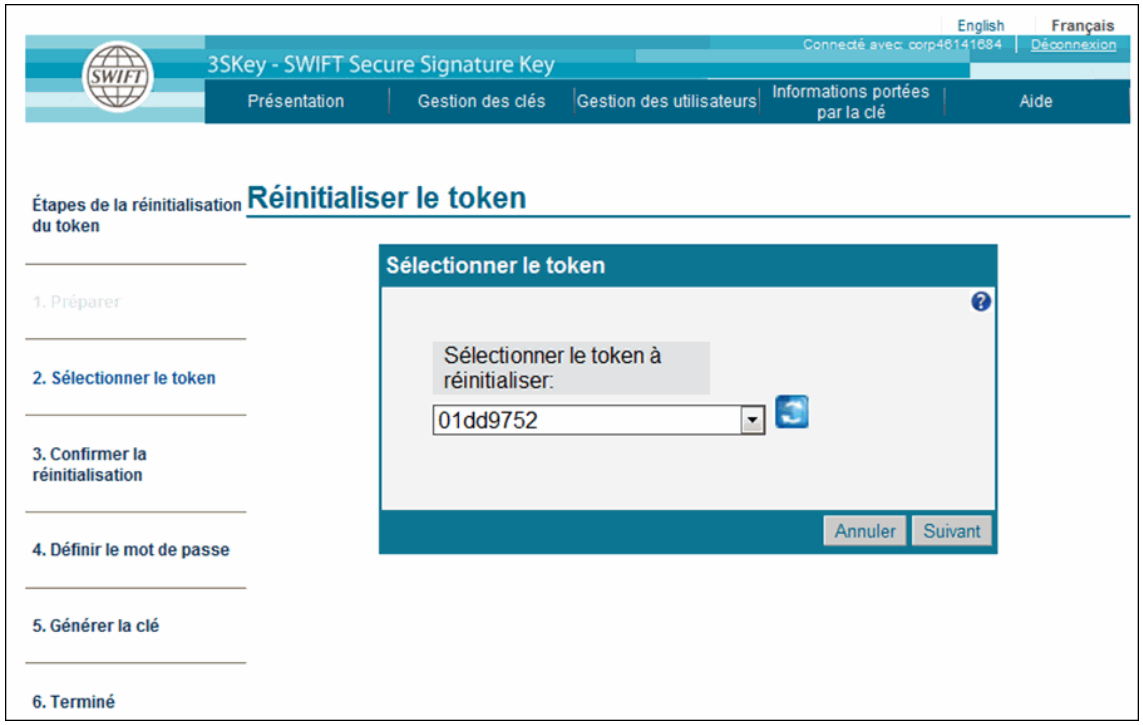
Notez que la colonne **Gestion des utilisateurs** n'apparaît sur la page **Présentation** que si vous vous êtes connecté avec le rôle `admin`.

3. La fenêtre de **réinitialisation du token** s'affiche et explique dans quelles circonstances la réinitialisation du token peut être utilisée.

English
Français
Connecté avec: corp46141684
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Réinitialiser le token
1. Préparer
2. Sélectionner le token
3. Confirmer la réinitialisation
4. Définir le mot de passe
5. Générer la clé
6. Terminé
Préparation de la réinitialisation
La réinitialisation du token est utilisée pour:
Ré-émettre un certificat et définir un nouveau mot de passe sur un token verrouillé ou dont le mot de passe est perdu.
Réinitialiser toute configuration effectuée par un administrateur 3SKey sur un token non activé.
Sans retirer votre token administrateur, insérez le token à réinitialiser et cliquez sur Suivant.
Annuler
Suivant

Insérez le token que vous souhaitez réinitialiser et cliquez sur Suivant.

4. La fenêtre **Sélectionner le token** s'ouvre et affiche le numéro de série du token à réinitialiser.



Sélectionnez le numéro de série du token dans la liste déroulante et cliquez sur Suivant.

5. La fenêtre **Confirmation de la préparation en vue d'une réinitialisation** s'affiche et fournit les détails du token à réinitialiser.

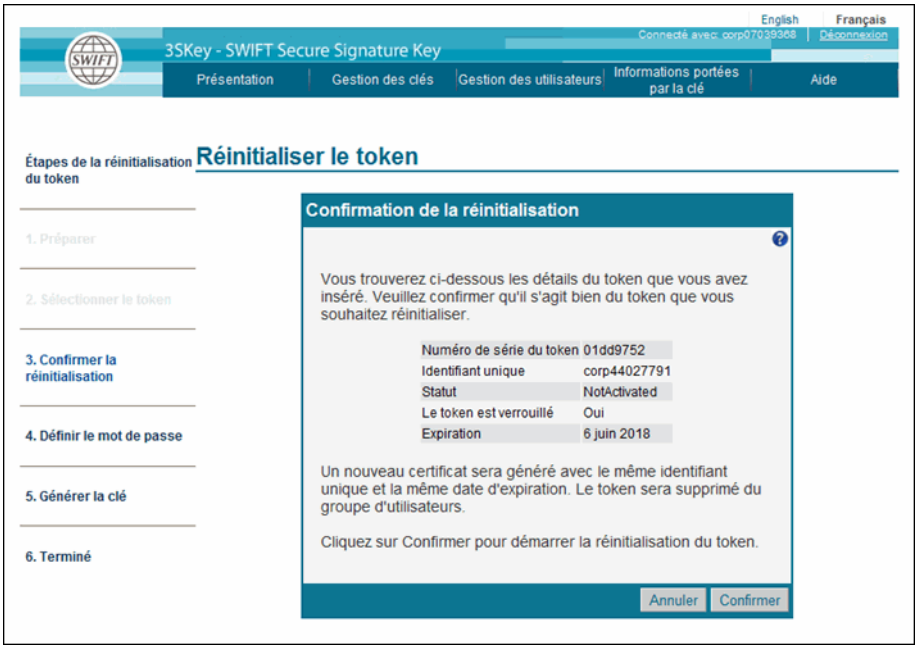
English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Configurer en vue d'une réinitialisation
1. Préparer
2. Sélectionner le token
3. Confirmer la réinitialisation
4. Définir le mot de passe
5. Générer la clé
6. Terminé
Confirmation de la préparation en vue d'une réinitialisation
Vous trouverez ci-dessous les détails du token que vous avez inséré. Veuillez confirmer qu'il s'agit bien du token que vous souhaitez réinitialiser.
Numéro de série du token 01dd9752
Identifiant unique corp44027791
Statut Activé (Réinitialisation interrompue)
Le token est verrouillé Non
Expiration 7 févr. 2017
Un nouveau certificat sera généré avec le même identifiant unique et la même date d'expiration. L'utilisateur du token a besoin du code de sécurité du token pour procéder à la réinitialisation.
Si vous confirmez cette étape, le certificat et le mot de passe sur ce token seront définitivement effacés.
Cliquez sur Confirmer pour démarrer la réinitialisation du token.
Annuler
Confirmer

Vérifiez le statut du token. Voici les scénarios possibles:

i. Si vous disposez d'un token dont le statut est **Activated** (Activé) qui ne se trouve pas en période de renouvellement (90 jours avant expiration), cliquez sur Confirmer et suivez la procédure décrite ici.

ii. Si vous disposez d'un token dont le statut est **Activated** (Activé) qui se trouve en période de renouvellement (90 jours avant expiration), vous devez configurer le token en vue d'une régénération. Pour ce faire, reportez-vous à la la section "Configurer un token en vue d'une régénération (pour les administrateurs)", page 67.

iii. Si vous disposez d'un token verrouillé dont le statut est **NotActivated** (Non activé) ou **Prepared to recover** (Préparé en vue d'une régénération), cliquez sur Confirmer et suivez la procédure décrite ici.


English
Français
Connecté avec: corp07035368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Réinitialiser le token
1. Préparer
2. Sélectionner le token
3. Confirmer la réinitialisation
4. Définir le mot de passe
5. Générer la clé
6. Terminé
Confirmation de la réinitialisation
Vous trouverez ci-dessous les détails du token que vous avez inséré. Veuillez confirmer qu'il s'agit bien du token que vous souhaitez réinitialiser.
Numéro de série du token 01dd9752
Identifiant unique corp44027791
Statut NotActivated
Le token est verrouillé Oui
Expiration 6 juin 2018
Un nouveau certificat sera généré avec le même identifiant unique et la même date d'expiration. Le token sera supprimé du groupe d'utilisateurs.
Cliquez sur Confirmer pour démarrer la réinitialisation du token.
Annuler
Confirmer

Remarque Si vous utilisez une ancienne version du logiciel 3SKey, il se peut qu'un token verrouillé soit incorrectement reporté comme non verrouillé. Ceci n'a aucun impact sur l'opération de réinitialisation. Veuillez vous reporter au Guide de dépannage 3SKey si vous souhaitez mettre à jour votre version du logiciel 3SKey vers la dernière version.

iv. Si vous disposez d'un token non verrouillé dont le statut est **NotActivated** (Non activé) ou **Prepared to recover** (Préparé en vue d'une régénération), la fenêtre **Confirmation de la réinitialisation** propose deux options:

   a. `Je ne connais pas le mot de passe du token` - dans ce cas, vous devez procéder à une réinitialisation complète qui supprimera du token toutes les informations relatives au certificat et génèrera un nouveau certificat technique.

      Sélectionnez l'option de mot de passe appropriée, cliquez sur Confirmer et suivez la procédure décrite ici.

   b. `Je connais le mot de passe du token` - dans ce cas, vous pouvez procéder à une réinitialisation rapide et garder le même certificat technique.

      Sélectionnez l'option de mot de passe appropriée, cliquez sur Confirmer et suivez la procédure décrite ici.

English
Français
Connecté avec: corp46141684
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Réinitialiser le token
1. Préparer
2. Sélectionner le token
3. Confirmer la réinitialisation
4. Définir le mot de passe
5. Générer la clé
6. Terminé
Confirmation de la réinitialisation
Vous trouverez ci-dessous les détails du token que vous avez inséré. Veuillez confirmer qu'il s'agit bien du token que vous souhaitez réinitialiser.
Numéro de série du token 01dd9752
Identifiant unique corp44027791
Statut NotActivated
Le token est verrouillé Non
Expiration 6 juin 2018
Je ne connais pas le mot de passe du token
Je connais le mot de passe du token
Annuler
Confirmer

Réinitialiser un token dont le statut est Activated (Activé)

La procédure de réinitialisation d'un token activé se déroule en deux étapes:

1. L'administrateur doit configurer le token en vue d'une réinitialisation.
2. L'utilisateur du token peut ensuite réinitialiser le token.

Important Avant de configurer un token pour sa réinitialisation, vérifiez que le propriétaire du token à réinitialiser dispose du code de sécurité de ce token.

Si vous ne disposez pas de votre code de sécurité, vous ne pouvez pas réinitialiser le token et vous devez activer un nouveau token avec un identifiant unique différent. Un token qui a été configuré en vue d'une réinitialisation dont le code de sécurité a été perdu est inutilisable.

Le code de sécurité a été téléchargé dans un fichier lors de l'activation du token. Par défaut, le nom du fichier est **code.txt** et il est stocké dans le dossier par défaut de votre navigateur.

Lorsque vous réinitialisez un token activé, la procédure est similaire à celle de la régénération d'un token sauf que, dans le cas d'une réinitialisation, vous utilisez le même token et non un nouveau token.

Configurer le token en vue d'une réinitialisation

1. En cliquant sur Confirmer, la fenêtre **Réinitialiser le mot de passe** s'ouvre.

English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
1. Préparer
2. Sélectionner le token
3. Confirmer la réinitialisation
4. Définir le mot de passe
5. Générer la clé
6. Terminé
Configurer en vue d'une réinitialisation
Réinitialiser le mot de passe
Sélectionnez un nouveau mot de passe pour le token à réinitialiser.
Les règles pour les mots de passe sont les suivantes:
• La longueur minimale est de quatre caractères.
• Caractères autorisés 0..9 A..Z a..z !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ et espace.
• Vous devez utiliser au moins deux caractères différents.
Nouveau mot de passe
Confirmation du nouveau mot de passe
Assurez-vous de vous souvenir du nouveau mot de passe. Sans ce mot de passe, vous ne serez pas en mesure d'accéder au token..
Annuler
Suivant

Introduisez un nouveau mot de passe en respectant les règles qui apparaissent à l'écran. Ré-introduisez le mot de passe et cliquez sur Suivant.

Remarque Veuillez noter que ce mot de passe devra à nouveau être modifié lorsque l'utilisateur finalisera la réinitialisation.

---

2. La page **Générer la clé** s'ouvre.

English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
1. Préparer
2. Sélectionner le token
3. Confirmer la réinitialisation
4. Définir le mot de passe
5. Générer la clé
6. Terminé
Configurer en vue d'une réinitialisation
Votre token est en cours de préparation pour la réinitialisation.
Ne retirez aucun des tokens du PC durant cette opération.
Initialiser le token
Générer la clé et demander la certification
Obtenir le certificat auprès de SWIFT
Enregistrer le nouveau certificat sur le token
Confirmer la réinitialisation du token à SWIFT

Cette étape génère un nouveau certificat technique avec le même identifiant unique que le certificat précédent et le stocke sur le token. Le statut du token passe à **Prepared to Reset** (Préparé en vue d'une réinitialisation).

Important Ce processus peut prendre quelques secondes. N'annulez pas l'opération en fermant le navigateur ou en déconnectant le token. Le token risquerait de devenir inutilisable.

Si le portail ne répond plus pendant plus de 5 minutes (en raison d'un problème de réseau), vous devez redémarrer le navigateur et ré-essayer l'opération.

3. La fenêtre **Configuration en vue de la réinitialisation terminée** s'ouvre.

   Lorsque la configuration est terminée, vous recevrez une confirmation indiquant que l'identifiant unique du token a été réinitialisé.

English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Configurer en vue d'une réinitialisation
1. Préparer
2. Sélectionner le token
3. Confirmer la réinitialisation
4. Définir le mot de passe
5. Générer la clé
6. Terminé
Configuration en vue de la réinitialisation terminée
Le token 01dd9752 a été préparé en vue d'une réinitialisation. Veuillez fournir le token et son nouveau mot de passe initial à l'utilisateur du token.
L'utilisateur du token doit se connecter au portail 3SKey à l'aide du token afin de terminer la procédure de réinitialisation.
Terminer

   Cliquez sur Terminer.

4. Le token apparaît dans le groupe d'utilisateurs avec le statut **Prepared to Reset** (Préparé en vue d'une réinitialisation).

   L'administrateur doit ensuite transférer le token avec le statut **Prepared to Reset** (Préparé en vue d'une réinitialisation) et son mot de passe à l'utilisateur du token. L'utilisateur doit se connecter au portail et terminer la réinitialisation. Reportez-vous à la section "Réinitialiser un token" pour terminer la réinitialisation.

Réinitialiser un token verrouillé dont le statut est Not Activated (Non activé) ou Prepared to Recover (Préparé en vue d'une régénération)

1. En cliquant sur Confirmer, la fenêtre **Réinitialiser le mot de passe** s'ouvre.

   Introduisez un nouveau mot de passe en respectant les règles qui apparaissent à l'écran. Ré-introduisez le mot de passe et cliquez sur Suivant.

English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Configurer en vue d'une réinitialisation
1. Préparer
2. Sélectionner le token
3. Confirmer la réinitialisation
4. Définir le mot de passe
5. Générer la clé
6. Terminé
Réinitialiser le mot de passe
Sélectionnez un nouveau mot de passe pour le token à réinitialiser.
Les règles pour les mots de passe sont les suivantes:
• La longueur minimale est de quatre caractères.
• Caractères autorisés 0..9 A..Z a..z !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ et espace.
• Vous devez utiliser au moins deux caractères différents.
Nouveau mot de passe
Confirmation du nouveau mot de passe
Assurez-vous de vous souvenir du nouveau mot de passe. Sans ce mot de passe, vous ne serez pas en mesure d'accéder au token..
Annuler
Suivant

2. La page **Générer la clé** s'ouvre.

   Cette étape génère un nouveau certificat avec le même identifiant unique que le certificat précédent.

English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Configurer en vue d'une réinitialisation
Votre token est en cours de préparation pour la réinitialisation.
Ne retirez aucun des tokens du PC durant cette opération.
1. Préparer
2. Sélectionner le token
3. Confirmer la réinitialisation
4. Définir le mot de passe
5. Générer la clé
6. Terminé
Initialiser le token
Générer la clé et demander la certification
Obtenir le certificat auprès de SWIFT
Enregistrer le nouveau certificat sur le token
Confirmer la réinitialisation du token à SWIFT

Important

Ce processus peut prendre quelques secondes. N'annulez pas l'opération en fermant le navigateur ou en déconnectant le token. Le token risquerait de devenir inutilisable.

Si le portail ne répond plus pendant plus de 5 minutes (en raison d'un problème de réseau), vous devez redémarrer le navigateur et ré-essayer l'opération.

3. Après quelques instants, la fenêtre **Réinitialisation du token terminée** s'ouvre.

   Elle affiche le numéro de série du token qui a été réinitialisé.

English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Réinitialiser le token
1. Préparer
2. Sélectionner le token
3. Confirmer la réinitialisation
4. Définir le mot de passe
5. Générer la clé
6. Terminé
Réinitialisation du token terminée
Le token 01dd9752 a été réinitialisé avec succès au statut non activé par défaut.
Il peut maintenant être ajouté à un groupe d'utilisateurs et assigné à un utilisateur.
Terminer

   Cliquez sur Terminer et la page **Présentation** s'ouvre.

   Au cours de cette procédure, le token est retiré du groupe d'utilisateurs. Et le statut du token passe de **Prepared to recover** (Préparé en vue d'une régénération) à **Not Activated** (Non activé).

   Le token peut maintenant être ajouté à un groupe d'utilisateurs et activé.

Réinitialiser un token non verrouillé dont le statut est Not Activated (Non activé) ou Prepared to Recover (Préparé en vue d'une régénération)

Si vous connaissez le mot de passe du token, procédez comme suit:

1. Cliquez sur `Je connais le mot de passe du token`.

English
Français
Connecté avec: corp46141684
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Réinitialiser le token
1. Préparer
2. Sélectionner le token
3. Confirmer la réinitialisation
4. Définir le mot de passe
5. Générer la clé
6. Terminé
Confirmation de la réinitialisation
Vous trouverez ci-dessous les détails du token que vous avez inséré. Veuillez confirmer qu'il s'agit bien du token que vous souhaitez réinitialiser.
Numéro de série du token 01dd9752
Identifiant unique corp44027791
Statut NotActivated
Le token est verrouillé Non
Expiration 6 juin 2018
Je ne connais pas le mot de passe du token
Je connais le mot de passe du token
Le token sera supprimé du groupe d'utilisateurs.
Cliquez sur Confirmer pour démarrer la réinitialisation du token.
Annuler
Confirmer

Cliquez sur Confirmer.

2. La fenêtre **Réinitialisation du token terminée** s'ouvre et affiche le numéro de série du token qui a été réinitialisé.

   Après réinitialisation, le statut du token passe à **NotActivated** (Non activé) et le token n'appartient plus à un groupe d'utilisateurs.

English
Français
Connecté avec: corp46141684
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Réinitialiser le token
1. Préparer
2. Sélectionner le token
3. Confirmer la réinitialisation
4. Définir le mot de passe
5. Générer la clé
6. Terminé
Réinitialisation du token terminée
Le token 01dd9752 a été réinitialisé avec succès au statut non activé par défaut.
Il peut maintenant être ajouté à un groupe d'utilisateurs et assigné à un utilisateur.
Terminer

Cliquez sur Terminer.

Au cours de cette procédure, le token est retiré du groupe d'utilisateurs. Et le statut du token passe de **Prepared to recover** (Préparé en vue d'une régénération) à **NotActivated** (Non activé).

3. Vous pouvez maintenant ajouter le token à un groupe d'utilisateurs et l'activer.

Si vous ne connaissez pas le mot de passe du token, procédez comme suit:

1. Cliquez sur `Je ne connais pas le mot de passe du token`.

English
Français
Connecté avec: corp46141684
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Réinitialiser le token
1. Préparer
2. Sélectionner le token
3. Confirmer la réinitialisation
4. Définir le mot de passe
5. Générer la clé
6. Terminé
Confirmation de la réinitialisation
Vous trouverez ci-dessous les détails du token que vous avez inséré. Veuillez confirmer qu'il s'agit bien du token que vous souhaitez réinitialiser.
Numéro de série du token 01dd9752
Identifiant unique corp44027791
Statut NotActivated
Le token est verrouillé Non
Expiration 6 juin 2018
Je ne connais pas le mot de passe du token
Je connais le mot de passe du token
Un nouveau certificat sera généré avec le même identifiant unique et la même date d'expiration. Le token sera supprimé du groupe d'utilisateurs.
Cliquez sur Confirmer pour démarrer la réinitialisation du token.
Annuler
Confirmer

2. Cliquez sur Confirmer. La fenêtre **Réinitialiser le mot de passe** s'ouvre.

English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Configurer en vue d'une réinitialisation
1. Préparer
2. Sélectionner le token
3. Confirmer la réinitialisation
4. Définir le mot de passe
5. Générer la clé
6. Terminé
Réinitialiser le mot de passe
Sélectionnez un nouveau mot de passe pour le token à réinitialiser.
Les règles pour les mots de passe sont les suivantes:
• La longueur minimale est de quatre caractères.
• Caractères autorisés 0..9 A..Z a..z !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ et espace.
• Vous devez utiliser au moins deux caractères différents.
Nouveau mot de passe
Confirmation du nouveau mot de passe
Assurez-vous de vous souvenir du nouveau mot de passe. Sans ce mot de passe, vous ne serez pas en mesure d'accéder au token..
Annuler
Suivant

Introduisez un nouveau mot de passe en respectant les règles qui apparaissent à l'écran. Ré-introduisez le mot de passe et cliquez sur Suivant.

3. La page **Générer la clé** s'ouvre.

   Cette étape génère un nouveau certificat avec le même identifiant unique que le certificat précédent.

English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Configurer en vue d'une réinitialisation
Votre token est en cours de préparation pour la réinitialisation.
Ne retirez aucun des tokens du PC durant cette opération.
1. Préparer
Initialiser le token
2. Sélectionner le token
Générer la clé et demander la certification
3. Confirmer la réinitialisation
Obtenir le certificat auprès de SWIFT
Enregistrer le nouveau certificat sur le token
4. Définir le mot de passe
Confirmer la réinitialisation du token à SWIFT
5. Générer la clé
6. Terminé

Important Ce processus peut prendre quelques secondes. N'abandonnez pas l'opération en fermant le navigateur ou en déconnectant le token. Le token risquerait de devenir inutilisable.

Si le portail ne répond plus pendant plus de 5 minutes (en raison d'un problème de réseau), vous devez redémarrer le navigateur et ré-essayer l'opération.

4. La fenêtre **Réinitialisation du token terminée** s'ouvre.

English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Réinitialiser le token
Réinitialisation du token terminée
1. Préparer
Le token 01dd9752 a été réinitialisé avec succès au statut non activé par défaut.
2. Sélectionner le token
Il peut maintenant être ajouté à un groupe d'utilisateurs et assigné à un utilisateur.
3. Confirmer la réinitialisation
Terminer
4. Définir le mot de passe
5. Générer la clé
6. Terminé

Elle affiche le numéro de série du token qui a été réinitialisé.

Cliquez sur Terminer et la page **Présentation** s'ouvre.

Au cours de cette procédure, le token est retiré du groupe d'utilisateurs. Et le statut du token passe de **Prepared to recover** (Préparé en vue d'une régénération) à **Not Activated** (Non activé).

Le token peut maintenant être ajouté à un groupe d'utilisateurs et activé.

10 Réinitialiser un token

Conditions préalables

Avant de pouvoir réinitialiser votre token:

- Votre administrateur doit avoir configuré votre token en vue d'une réinitialisation, comme décrit dans la section "Configurer un token en vue d'une réinitialisation (pour les administrateurs)", page 43.
- Vous devez avoir reçu votre token et son nouveau mot de passe de votre administrateur.
- Vous devez disposer de votre code de sécurité.

Important Si vous ne disposez pas de votre code de sécurité, vous ne pouvez pas réinitialiser le token et vous devez activer un nouveau token avec un identifiant unique différent. Un token qui a été configuré en vue d'une réinitialisation dont le code de sécurité a été perdu est inutilisable.

Le format du code de sécurité est XXXX-XXXX-XXXX-XXXX. Le code est sensible à la casse. Le code de sécurité a été téléchargé dans un fichier lors de l'activation du token. Par défaut, le nom du fichier est **code.txt**.

Réinitialiser un token

Pour réinitialiser votre token qui a été **configuré en vue d'une ré-initialisation** par votre administrateur, procédez comme suit:

1. Connectez-vous au portail à l'aide du token qui doit être réinitialisé.
2. La fenêtre **Réinitialiser votre token** s'affiche automatiquement.

English
Français
3SKey - SWIFT Secure Signature Key
Connecté avec: corp44027791 | Déconnexion
Étapes de la réinitialisation du token
Réinitialiser votre token
1. Vérifier le code
Votre administrateur a préparé votre token pour la réinitialisation. Cette procédure terminera la réinitialisation de votre token.
2. Modifier le mot de passe
3. Générer la clé
4. Terminé
Annuler
Suivant

Cliquez sur Suivant.

3. La fenêtre **Valider le code de sécurité** s'ouvre. Introduisez le code de sécurité du token.

English
Français
Connecté avec: corp44027791 | Déconnexion
3SKey - SWIFT Secure Signature Key
Étapes de la réinitialisation du token
Valider le code de sécurité
Le portail validera le code de sécurité de l'identifiant unique à réinitialiser.
1. Vérifier le code
2. Modifier le mot de passe
3. Générer la clé
4. Terminé
Valider le code de sécurité
Entrez le code de sécurité de l'identifiant unique corp44027791
Code de sécurité:
Valider

Cliquez sur Valider.

4. La fenêtre **Modifier le mot de passe du token** s'ouvre.

English
Français
Connecté avec: corp44027791 | Déconnexion
3SKey - SWIFT Secure Signature Key
Étapes de la réinitialisation du token
Modifier le mot de passe du token
Vous devez modifier le mot de passe initial du token.
1. Vérifier le code
Assurez-vous de vous souvenir du nouveau mot de passe. Sans ce mot de passe, vous ne serez pas en mesure d'accéder au token..
2. Modifier le mot de passe
3. Générer la clé
4. Terminé
Modifier le mot de passe du token
Sélectionnez un nouveau mot de passe pour votre token.
Les règles pour les mots de passe sont les suivantes:
• La longueur minimale est de quatre caractères.
• Caractères autorisés 0..9 A..Z a..z !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ et espace.
• Vous devez utiliser au moins deux caractères différents.
• Vous ne pouvez pas réutiliser la valeur actuelle ou précédente du mot de passe.
Mot de passe actuel
Nouveau mot de passe
Confirmation du nouveau mot de passe
Modifier

Introduisez le mot de passe actuel du token, et introduisez ensuite un nouveau mot de passe pour le token en respectant les règles qui s'affichent à l'écran.

Confirmez le nouveau mot de passe et cliquez sur Modifier.

Vous recevrez une confirmation indiquant que le nouveau mot de passe a été modifié avec succès.

English
Français
Connecté avec corp44027791
Déconnexion
3SKey - SWIFT Secure Signature Key
Étapes de la réinitialisation du token
Modifier le mot de passe du token
1. Vérifier le code
Assurez-vous de vous souvenir du nouveau mot de passe. Sans ce mot de passe, vous ne serez pas en mesure d'accéder au token..
2. Modifier le mot de passe
Modifier le mot de passe du token
3. Générer la clé
Le mot de passe a été modifié avec succès
4. Terminé
Suivant

Cliquez sur Suivant.

5. La page **Générer la clé** s'affiche.

English
Français
Connecté avec corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Étapes de la réinitialisation du token
Générer la clé
Votre token est en cours de réinitialisation.
1. Vérifier le code
2. Modifier le mot de passe
Générer la clé et demander la certification
Obtenir le certificat auprès de SWIFT
Enregistrer le nouveau certificat sur le token
Confirmer la réinitialisation du token à SWIFT
3. Générer la clé
4. Terminé

La réinitialisation de la clé peut prendre quelques secondes. N'annulez pas l'opération en fermant le navigateur ou en déconnectant le token. Le token risquerait de devenir inutilisable.

Si le portail ne répond plus pendant plus de 5 minutes (en raison d'un problème de réseau), vous devez redémarrer le navigateur et ré-essayer l'opération. Vous devrez vous connecter en utilisant le nouveau mot de passe. Vous devrez à nouveau modifier le mot de passe dans la fenêtre **Modifier le mot de passe du token** (voir étape 4).

La fenêtre **Réinitialisation du token terminée** s'ouvre.

English
Français
Connecté avec: corp44027791
Déconnexion
3SKey - SWIFT Secure Signature Key
Étapes de la réinitialisation du token
Réinitialisation du token terminée
Votre token a été réinitialisé avec succès.
1. Vérifier le code
Cliquez sur Terminer, retirez votre token du PC et déconnectez-vous du portail 3SKey .
2. Modifier le mot de passe
3. Générer la clé
4. Terminé
Terminer

Cliquez sur Terminer.

Réinitialisation terminée

La réinitialisation de votre token est maintenant terminée et un nouveau certificat a été généré avec le même identifiant unique et la même date d'expiration que le certificat précédent. Votre token est maintenant prêt à l'emploi, toutefois - en fonction de la manière dont votre banque enregistre les tokens - il peut être nécessaire d'informer la banque de la réinitialisation.

Vous pouvez utiliser le token réinitialisé sur n'importe quel PC sur lequel le logiciel du token 3SKey est installé. Si vous souhaitez utiliser le token immédiatement sur le PC que vous avez utilisé pour l'activation, vous devez vous déconnecter du portail 3SKey et retirer le token du port USB.

Remarque Le code de sécurité du token reste valide. Si vous souhaitez remplacer le code de sécurité, reportez-vous à "Générer le code de sécurité", page 78.

11 Révoquer un token

Présentation

La révocation d'un token a les conséquences suivantes:

- La révocation du token rend non valides tous les certificats associés à l'identifiant unique du token.
- Une fois que le token a été révoqué, 3SKey l'ajoute à la liste de révocation des certificats. Les applications destinées à vérifier la liste de révocation des certificats ne considèrent alors plus les certificats correspondant à l'identifiant unique associé au token comme des certificats de confiance.
- Un token révoqué ne peut pas être réutilisé.

Révoquer un token est nécessaire si, par exemple, vous avez perdu le token, vous suspectez qu'il a été compromis, ou que l'utilisateur du token a quitté votre organisation.

Si vous souhaitez continuer à utiliser l'identifiant unique qui se trouvait sur le token d'origine, vous devez régénérer cet identifiant. Le processus de régénération révoque automatiquement le token d'origine. Pour de plus amples informations, reportez-vous à "Configurer un token en vue d'une régénération (pour les administrateurs)", page 67 et "Régénérer un token", page 70.

Si vous révoquez un token ayant le rôle `admin`, il peut être nécessaire de régénérer l'identifiant unique ou de configurer un nouveau token, afin que votre organisation ait toujours au moins deux tokens d'administrateur.

Remarque Il est impossible de révoquer un token non activé.

Lorsqu'une opération requiert que vous fournissiez deux informations différentes, vous devez fournir la seconde information dans les **cinq minutes** suivant la première. Sinon, votre session peut arriver à expiration et vous devez recommencer le processus de révocation.

Comment révoquer un token

Il existe trois moyens pour révoquer un token activé:

- Se connecter avec le token suspect et le révoquer. Voir "Méthode 1: Révoquer le token avec lequel vous vous êtes connecté".
- Se connecter en tant qu'administrateur du groupe d'utilisateurs auquel le token appartient, et révoquer le token suspect. Voir "Méthode 2: Révoquer un token en tant qu'administrateur".
- Dans des situations exceptionnelles, si la méthode 1 et la méthode 2 ne sont pas possibles, vous pouvez vous connecter avec un token non activé et révoquer le token suspect. Par exemple, vous pouvez utiliser cette troisième méthode s'il est nécessaire de révoquer un token perdu en urgence en l'absence des administrateurs.

  Pour utiliser cette méthode, vous avez besoin du code de sécurité du token que vous souhaitez révoquer. Le code de sécurité a été téléchargé dans un fichier lors de l'activation du token. Par défaut, le nom du fichier est **code.txt**.

  Voir "Méthode 3: Utiliser un token non activé pour révoquer un token".

Remarque Si vous devez révoquer un token qui a été renouvelé, vous aurez la possibilité de révoquer l'ancien ou le nouveau token lorsque vous sélectionnez l'identifiant unique comme indiqué dans l'exemple suivant.

Méthode 1: Révoquer le token avec lequel vous vous êtes connecté

1. Connectez-vous au portail 3SKey avec le token que vous souhaitez révoquer.
2. Dans la colonne **Gestion des clés**, cliquez sur **Révoquer**.

   3SKey affiche votre identifiant unique.

   Effectuez la procédure de révocation en suivant les étapes décrites dans la section "Terminer la révocation du token".

Méthode 2: Révoquer un token en tant qu'administrateur

1. Connectez-vous au portail 3SKey en utilisant un token `admin` du même groupe d'utilisateurs que celui du token devant être révoqué.
2. Dans la colonne **Gestion des clés**, cliquez sur **Révoquer**.
3. Sélectionnez l'identifiant unique que vous souhaitez révoquer dans la liste déroulante.

   Cette liste contient tous les tokens qui sont membres du groupe d'utilisateurs auquel le token administrateur appartient.

   Effectuez la procédure de révocation en suivant les étapes décrites dans la section "Terminer la révocation du token".

Méthode 3: Utiliser un token non activé pour révoquer un token

1. Connectez-vous au portail 3SKey en utilisant un token non activé.

   3SKey affiche la page **Activation du token**.

2. Cliquez sur Annuler.

   La page principale du portail 3SKey s'affiche.

3. Dans la colonne **Gestion des clés**, cliquez sur **Révoquer**.

4. Entrez l'identifiant unique et le code de sécurité du token que vous souhaitez révoquer.

   Le format du code de sécurité est XXXX-XXXX-XXXX-XXXX. Le code est sensible à la casse.

   Effectuez la procédure de révocation en suivant les étapes décrites dans la section "Terminer la révocation du token".

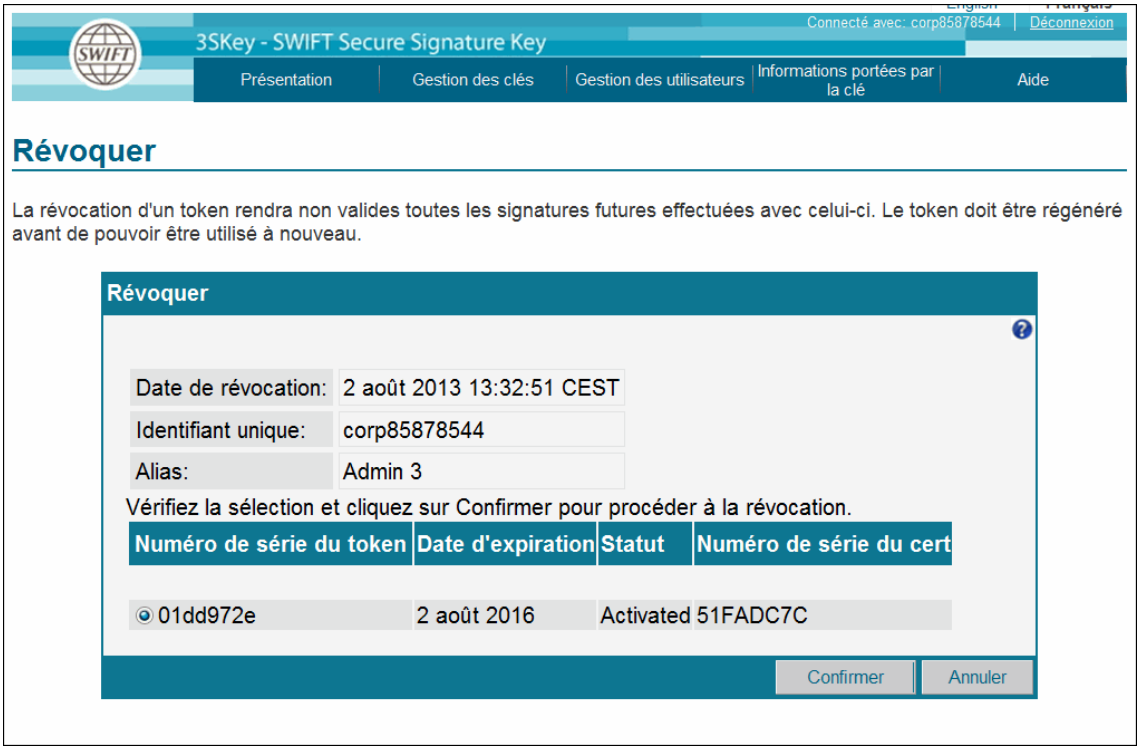
Terminer la révocation du token

Suivez les étapes décrites dans la Méthode 1, 2, ou 3 et terminez la procédure de révocation comme suit:

1. Cliquez sur Soumettre.

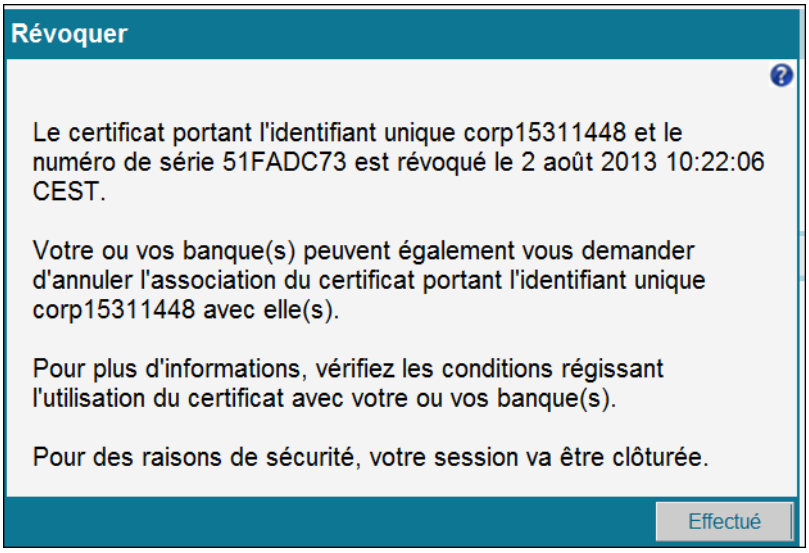
   3SKey affiche les informations relatives à votre identifiant unique. La **Date de révocation** est l'horodatage sur le serveur. L'**Identifiant unique** est l'utilisateur que vous souhaitez révoquer.

   Si votre token a été renouvelé, vous verrez 2 certificats avec le même identifiant unique et vous serez en mesure de sélectionner l'ancien ou le nouveau token.



2. Vérifiez que l'**identifiant unique** affiché est celui que vous souhaitez révoquer et cliquez sur Confirmer.

3. Le portail affiche une confirmation indiquant que la révocation du token a réussi.


Révoquer
Le certificat portant l'identifiant unique corp15311448 et le numéro de série 51FADC73 est révoqué le 2 août 2013 10:22:06 CEST.
Votre ou vos banque(s) peuvent également vous demander d'annuler l'association du certificat portant l'identifiant unique corp15311448 avec elle(s).
Pour plus d'informations, vérifiez les conditions régissant l'utilisation du certificat avec votre ou vos banque(s).
Pour des raisons de sécurité, votre session va être clôturée.
Effectué

Cliquez sur Effectué. Si vous utilisez la Méthode 1, votre session est clôturée.

12 Configurer un token en vue d'une régénération (pour les administrateurs)

Qu'est-ce que la régénération et quand l'utiliser

Le processus de régénération vous permet de réutiliser l'identifiant unique d'un ancien token et de l'associer à un autre token. Pour utiliser le processus de régénération, vous devez disposer du code de sécurité du token d'origine et votre administrateur doit avoir configuré un nouveau token en vue d'une régénération.

Si possible, vous devez utiliser le processus de régénération dans les situations suivantes:

- Si un token est perdu ou endommagé
- Si le token a expiré
- Si le token a été révoqué

Remarque La régénération nécessite le code de sécurité du token. Si vous ne disposez pas de votre code de sécurité, vous devez activer un nouveau token avec un identifiant unique différent.

Quand ne pas utiliser la régénération

Dans les cas suivants, le token doit être réinitialisé:

- Si le propriétaire du token a oublié le mot de passe
- Si le propriétaire a verrouillé le token en entrant cinq mots de passe incorrects consécutifs

Remarque Si un token à réinitialiser se trouve en période de renouvellement (90 jours avant expiration) vous ne pouvez pas le réinitialiser et vous devez le régénérer sur un nouveau token. Si vous ne disposez pas de votre code de sécurité, vous ne pouvez pas réinitialiser ni régénérer le token et vous devez activer un nouveau token avec un identifiant unique différent.

Il est impossible de régénérer un token non activé.

Présentation de la régénération

Vous pouvez utiliser cette page pour préparer la régénération d'un token qui est inutilisable. Cette page est disponible uniquement lorsque vous vous êtes connecté avec un token ayant le rôle `admin`.

Le token peut être inutilisable pour l'une des raisons suivantes:

- Le token est perdu ou compromis
- Le token a été révoqué
- Le token a expiré

Cette page vous permet d'attribuer un token non activé en remplacement du token d'origine.

Il est impossible de régénérer un token non activé.

Lorsque le propriétaire a régénéré le token d'origine, le nouveau token aura les caractéristiques suivantes:

- L'identifiant unique du token d'origine.

  Celui-ci remplace l'identifiant unique qui était sur le nouveau token non activé.

- Le rôle du token d'origine.
- L'alias du token d'origine.
- Un certificat métier qui comporte l'identifiant d'objet du certificat métier d'origine, mais un nouveau numéro de série.
- Une date d'expiration définie trois ans après l'opération de régénération.

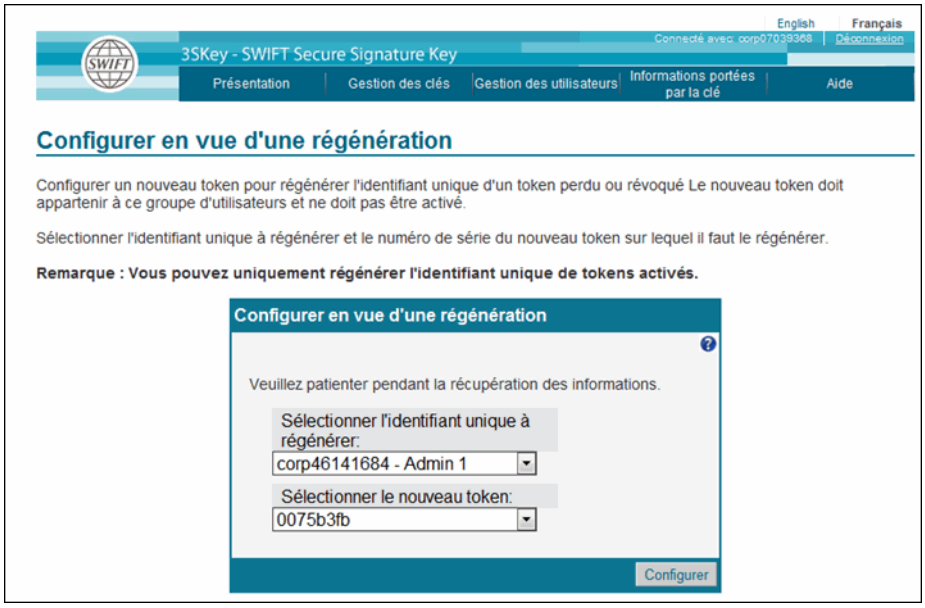
Pour plus d'informations sur ces caractéristiques, reportez-vous à "Informations portées par la clé - détails du certificat et du token", page 79.

Important Avant de configurer un token pour sa régénération, vérifiez que le propriétaire du token à régénérer dispose du code de sécurité de ce token.

Sans le code de sécurité, le token que vous avez configuré en vue d'une régénération ne peut pas être utilisé pour régénérer cet identifiant unique particulier. Vous pouvez réinitialiser le token configuré en vue d'une régénération afin de le faire revenir à son état d'origine non activé.

Le code de sécurité a été téléchargé dans un fichier lors de l'activation du token. Par défaut, le nom du fichier est **code.txt**.

Écran


English
Français
Connecté avec: corp07039368
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Gestion des utilisateurs
Informations portées par la clé
Aide
Configurer en vue d'une régénération
Configurer un nouveau token pour régénérer l'identifiant unique d'un token perdu ou révoqué Le nouveau token doit appartenir à ce groupe d'utilisateurs et ne doit pas être activé.
Sélectionner l'identifiant unique à régénérer et le numéro de série du nouveau token sur lequel il faut le régénérer.
Remarque : Vous pouvez uniquement régénérer l'identifiant unique de tokens activés.
Configurer en vue d'une régénération
Veuillez patienter pendant la récupération des informations.
Sélectionner l'identifiant unique à régénérer:
corp46141684 - Admin 1
Sélectionner le nouveau token:
0075b3fb
Configurer

Champs

Sélectionner l'identifiant unique à régénérer

La liste déroulante contient l'identifiant unique et l'alias (le cas échéant) de chaque token activé dans votre groupe d'utilisateurs. Sélectionnez l'identifiant unique à régénérer.

Sélectionner le nouveau token

La liste déroulante contient les numéros de série de tous les tokens non activés ayant été ajoutés au groupe d'utilisateurs. Ils sont disponibles pour la régénération du token inutilisable.

Sélectionnez le numéro de série qui est imprimé sur le token que vous souhaitez utiliser.

Si le token que vous souhaitez utiliser ne se trouve pas dans la liste, ajoutez-le au groupe d'utilisateurs. Pour plus d'informations, reportez-vous à "Ajouter un utilisateur à un groupe d'utilisateurs (pour les administrateurs)", page 18.

Terminer la configuration

Cliquer sur Effectué

Lorsque tous les champs sont renseignés correctement, cliquez sur Effectué pour terminer la configuration.

Transférer le token

Lorsque la configuration est terminée, transférez le nouveau token au propriétaire du token devant être régénéré.

Assurez-vous que le propriétaire dispose également du mot de passe d'activation que votre banque a fourni avec le token.

Pour plus d'informations sur le processus de régénération, reportez-vous à "Régénérer un token", page 70.

13 Régénérer un token

Qu'est-ce que la régénération et quand l'utiliser

Le processus de régénération vous permet de réutiliser l'identifiant unique d'un ancien token et de l'associer à un autre token. Pour utiliser le processus de régénération, vous devez disposer du code de sécurité du token d'origine et votre administrateur doit avoir configuré un nouveau token en vue d'une régénération.

Si possible, vous devez utiliser le processus de régénération dans les situations suivantes:

- Si un token est perdu ou endommagé
- Si le token a expiré
- Si le token a été révoqué

Remarque La régénération nécessite le code de sécurité du token. Si vous ne disposez pas de votre code de sécurité, vous devez activer un nouveau token avec un identifiant unique différent.

Quand ne pas utiliser la régénération

Dans les cas suivants, le token doit être réinitialisé:

- Si le propriétaire du token a oublié le mot de passe
- Si le propriétaire a verrouillé le token en entrant cinq mots de passe incorrects consécutifs

Remarque Si votre token est verrouillé et qu'il se trouve en période de renouvellement, vous ne pouvez pas réinitialiser votre token et vous devez le régénérer. Si vous ne disposez pas de votre code de sécurité, vous ne pouvez pas réinitialiser ni régénérer le token et vous devez activer un nouveau token avec un identifiant unique différent.

Si votre token n'est pas encore activé, il n'est pas possible de le régénérer.

Présentation de la régénération

La procédure de régénération se déroule en 2 parties:

1. Un utilisateur avec le rôle `admin` configure un token de réserve pour la régénération. Pour des informations complémentaires, reportez-vous à "Configurer un token en vue d'une régénération (pour les administrateurs)", page 67.
2. L'utilisateur de l'ancien token se connecte avec le token de réserve préparé, fournit le code de sécurité et modifie le mot de passe. Reportez-vous à la section "Procédure de régénération" ci-dessous.

Remarque Durant la régénération, le portail 3SKey configure le nouveau token pour qu'il ait l'identifiant unique du token d'origine. Dans le cadre de ce processus, le portail révoque le certificat sur l'ancien token. L'ancien token ne peut par conséquent plus être utilisé.

Procédure de régénération

1. Connectez-vous au portail 3SKey avec un token ayant été configuré en vue d'une régénération.

English
Français
Connecté avec: corp57585058
Déconnexion
3SKey - SWIFT Secure Signature Key
Étapes de la régénération
Régénérer
1. Vérifier le code
2. Modifier le mot de passe
3. Générer la clé
4. Terminé
Ce nouveau token a été configuré par votre administrateur pour régénérer votre identifiant unique. Vous devez fournir le code de sécurité associé à votre identifiant unique pour terminer le processus de régénération..
Annuler
Suivant

   À ce stade, l'identifiant unique et le mot de passe d'origine du token sont toujours associés au token. Le processus de régénération remplace l'identifiant unique par celui que vous régénérez.

   Dans le champ **Mot de passe**, indiquez le mot de passe initial qui accompagnait le token avec lequel vous êtes connecté.

2. Cliquez sur Suivant.

   Le portail 3SKey affiche une page contenant les informations relatives à l'identifiant unique pour lequel le token de réserve a été configuré.

English
Français
Connecté avec: corp57585058
Déconnexion
3SKey - SWIFT Secure Signature Key
Étapes de la régénération
Valider le code de sécurité
Le portail validera le code de sécurité de l'identifiant unique à régénérer.
1. Vérifier le code
2. Modifier le mot de passe
3. Générer la clé
4. Terminé
Valider le code de sécurité
Entrez le code de sécurité de l'identifiant unique corp07039368
Code de sécurité:
Valider

3. Vérifiez que l'identifiant unique affiché est celui que vous souhaitez régénérer et entrez le code de sécurité associé à cet identifiant unique. Les caractères sont masqués et ne sont donc pas visibles.

Remarque

Le format du code de sécurité est `XXXX-XXXX-XXXX-XXXX`. Le code est sensible à la casse.

Le code de sécurité a été téléchargé dans un fichier lors de l'activation du token. Par défaut, le nom du fichier est **code.txt**.

4. Cliquez sur Valider pour vérifier que le code de sécurité correspond à l'identifiant unique régénéré.

5. Vous devez maintenant modifier le mot de passe. Saisissez un nouveau mot de passe dans la zone d'édition **Nouveau mot de passe**, confirmez le mot de passe en le saisissant à nouveau dans la zone d'édition **Confirmation du nouveau mot de passe** et cliquez sur Modifier.

English
Français
Connecté avec: corp57585058
Déconnexion
3SKey - SWIFT Secure Signature Key
Étapes de la régénération
1. Vérifier le code
2. Modifier le mot de passe
3. Générer la clé
4. Terminé
Modifier le mot de passe du token
Vous devez modifier le mot de passe initial du token.
Assurez-vous de vous souvenir du nouveau mot de passe. Sans ce mot de passe, vous ne serez pas en mesure d'accéder au token..
Modifier le mot de passe du token
Sélectionnez un nouveau mot de passe pour votre token.
Les règles pour les mots de passe sont les suivantes:
• La longueur minimale est de quatre caractères.
• Caractères autorisés 0..9 A..Z a..z !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ et espace.
• Vous devez utiliser au moins deux caractères différents.
• Vous ne pouvez pas réutiliser la valeur actuelle ou précédente du mot de passe.
Mot de passe actuel
Nouveau mot de passe
Confirmation du nouveau mot de passe
Modifier

Fournissez un mot de passe sécurisé. Suivez les directives ci-après lorsque vous créez un mot de passe:

- La longueur minimale est de quatre caractères
- La longueur maximale est de seize caractères
- Vous pouvez utiliser les caractères suivants:

  – `0-9 A-Z a-z` et espace

  – `! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~`

- Vous devez utiliser au moins deux caractères différents. Par exemple, vous ne pouvez pas définir le mot de passe sur `aaaa` ou `11111`
- Vous ne pouvez pas utiliser de caractères accentués (é ou ö par exemple)
- Vous ne pouvez pas ré-utiliser le mot de passe initial qui accompagnait le nouveau token

La page **Modifier le mot de passe du token** apparaît avec le texte `Le mot de passe a été modifié avec succès`.

English
Français
Connecté avec: corp57585058
Déconnexion
3SKey - SWIFT Secure Signature Key
Étapes de la régénération
Modifier le mot de passe du token
1. Vérifier le code
Assurez-vous de vous souvenir du nouveau mot de passe. Sans ce mot de passe, vous ne serez pas en mesure d'accéder au token..
2. Modifier le mot de passe
Modifier le mot de passe du token
3. Générer la clé
Le mot de passe a été modifié avec succès
4. Terminé
Suivant

6. Cliquez sur Suivant.

   3SKey génère la clé.

   Une fois que l'opération a été effectuée avec succès, l'identifiant unique de l'ancien token est recréé sur le nouveau token.

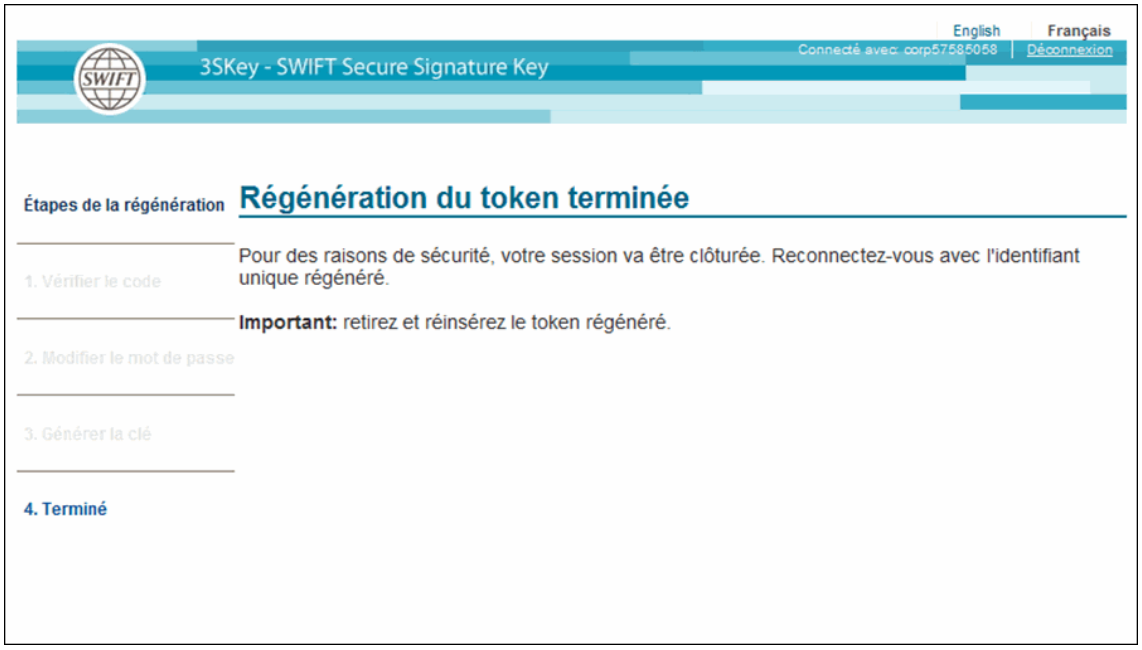
English
Français
Connecté avec: corp57585058
Déconnexion
3SKey - SWIFT Secure Signature Key
Étapes de la régénération
Générer la clé
1. Vérifier le code
Veuillez patienter pendant la régénération de votre identifiant unique sur le nouveau token.
Générer la clé et demander la certification
2. Modifier le mot de passe
Obtenir le certificat auprès de SWIFT
Enregistrer le nouveau certificat sur le token
3. Générer la clé
Confirmer la régénération du token à SWIFT
4. Terminé

Important La génération de la clé peut prendre quelques secondes. N'annulez pas l'opération en fermant le navigateur ou en déconnectant le token. Le token risquerait de devenir inutilisable.

Si le portail ne répond plus pendant plus de 5 minutes (en raison d'un problème de réseau), vous devez redémarrer le navigateur et ré-essayer l'opération. Veuillez noter que le mot de passe sur le nouveau token aura été modifié. Vous devrez à nouveau le modifier dans la fenêtre **Modifier le mot de passe du token** (voir étape 5).

Régénération terminée

La régénération de votre identifiant unique est maintenant terminée et vous pouvez utiliser le nouveau token pour authentifier des transactions commerciales. Toutefois - en fonction de la manière dont votre banque enregistre les tokens - il peut être nécessaire d'informer la banque du remplacement.


English
Français
Connecté avec: corp57585058
Déconnexion
3SKey - SWIFT Secure Signature Key
Étapes de la régénération
Régénération du token terminée
1. Vérifier le code
Pour des raisons de sécurité, votre session va être clôturée. Reconnectez-vous avec l'identifiant unique régénéré.
Important: retirez et réinsérez le token régénéré.
2. Modifier le mot de passe
3. Générer la clé
4. Terminé

Vous pouvez utiliser le nouveau token sur n'importe quel PC sur lequel les pilotes de token 3SKey sont installés. Si vous souhaitez utiliser le token immédiatement sur le PC que vous avez utilisé pour l'activation, vous devez vous déconnecter du portail 3SKey et retirer le token du port USB. (S'il s'agit d'un token 3SKey NG-FLASH, utilisez l'icône sur la barre des tâches **Retirer le matériel en toute sécurité** .) Réinsérez ensuite le token dans le port USB: cette opération ajoute les informations sur le certificat du nouveau token dans le magasin des certificats.

Remarque Le code de sécurité du token d'origine reste valide. Si vous souhaitez remplacer le code de sécurité, reportez-vous à "Générer le code de sécurité", page 78.

14 Mot de passe

14.1 Règles en matière de mot de passe

Présentation

Le token est protégé par un mot de passe. Vous utilisez ce mot de passe aussi bien pour vous connecter au portail 3SKey que pour signer vos transactions.

Important Le mot de passe n'expire pas, mais SWIFT recommande de le modifier tous les trois mois.

Pour modifier le mot de passe, assurez-vous d'être connecté avec le token pour lequel vous souhaitez modifier le mot de passe. Cliquez ensuite sur le menu **Gestion des clés** et sélectionnez l'élément **Modifier le mot de passe**.

Règles en matière de mot de passe

Fournissez un mot de passe sécurisé. Suivez les directives ci-après lorsque vous créez un mot de passe:

- La longueur minimale est de quatre caractères
- La longueur maximale est de seize caractères
- Vous pouvez utiliser les caractères suivants:

  – `0-9 A-Z a-z` et espace

  – `! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~`

- Vous devez utiliser au moins deux caractères différents. Par exemple, vous ne pouvez pas définir le mot de passe sur `aaaa` ou `11111`
- Vous ne pouvez pas utiliser de caractères accentués (é ou ö par exemple)
- Vous ne pouvez pas réutiliser le mot de passe actuel ni le mot de passe précédent

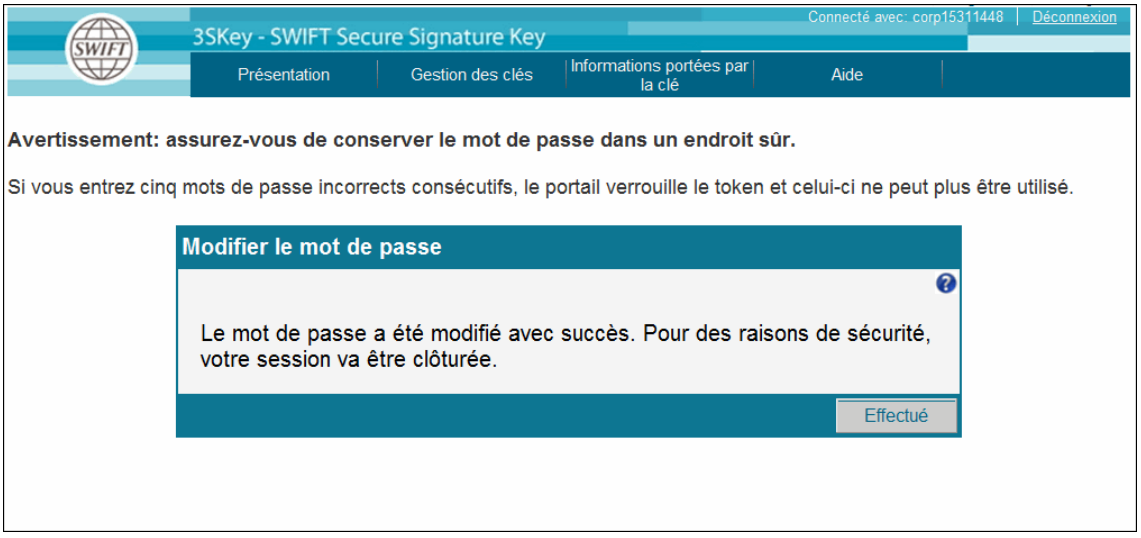
14.2 Comment modifier le mot de passe

Modifier le mot de passe

1. Connectez-vous au portail 3SKey avec le token dont vous souhaitez modifier le mot de passe.
2. Sur la page **Présentation**, cliquez sur **Modifier le mot de passe**.

   La page **Modifier le mot de passe** apparaît.
3. Saisissez le nouveau mot de passe dans la zone d'édition **Nouveau mot de passe**.
4. Confirmez le mot de passe en le saisissant à nouveau dans la zone d'édition **Confirmation du nouveau mot de passe**.
5. Cliquez sur Modifier.

La page **Modifier le mot de passe** apparaît avec le texte `Le mot de passe a été modifié avec succès`.


Connecté avec: corp15311448
Déconnexion
3SKey - SWIFT Secure Signature Key
Présentation
Gestion des clés
Informations portées par la clé
Aide
Avertissement: assurez-vous de conserver le mot de passe dans un endroit sûr.
Si vous entrez cinq mots de passe incorrects consécutifs, le portail verrouille le token et celui-ci ne peut plus être utilisé.
Modifier le mot de passe
Le mot de passe a été modifié avec succès. Pour des raisons de sécurité, votre session va être clôturée.
Effectué

6. Cliquez sur Effectué.

   Le token est maintenant protégé par le nouveau mot de passe.

Mot de passe perdu ou incorrect

Si vous perdez ou que vous oubliez votre mot de passe, ou que votre token se verrouille après saisie de cinq mots de passe incorrects, contactez votre administrateur.

15 Générer le code de sécurité

Présentation

Le code de sécurité est utilisé pour:

- Régénérer l'identifiant unique d'un token expiré, perdu, endommagé ou révoqué sur un nouveau token. Pour des informations complémentaires sur la régénération, reportez-vous à "Régénérer un token", page 70.
- Révoquer un token en utilisant un token non activé si ni le propriétaire du token ni l'administrateur ne peut le révoquer. Pour des informations complémentaires sur la révocation, reportez-vous à "Révoquer un token", page 63.
- Réinitialiser un token activé qui est verrouillé ou dont le mot de passe est perdu et qui a été configuré en vue d'une réinitialisation. Pour des informations complémentaires sur la réinitialisation, reportez-vous à "Configurer un token en vue d'une réinitialisation (pour les administrateurs)", page 43.

Pour générer un nouveau code de sécurité, par exemple car vous l'avez perdu, connectez-vous au portail 3SKey en utilisant le token pour lequel vous souhaitez régénérer un code de sécurité, cliquez sur le menu **Gestion des clés** et sélectionnez **Générer le code de sécurité**.

Si un token est inutilisable car il est verrouillé, perdu, révoqué ou expiré et si le code de sécurité a été perdu, il n'est pas possible de réinitialiser ni de régénérer le token et un nouveau token doit être activé.

Procédure

1. Cliquez sur Générer.
2. Cliquez sur Télécharger pour enregistrer le code de sécurité dans un fichier.

   Le portail vous invite à enregistrer le fichier, avec le nom **code.txt** dans le dossier par défaut de votre navigateur. Le cas échéant, vous pouvez modifier le nom du fichier et le dossier.
3. Cliquez sur Confirmer.

Important Le code de sécurité généré est effectif seulement après que vous avez cliqué sur Confirmer et obtenu une confirmation positive du serveur. Vous devez cliquer sur Confirmer dans les cinq minutes après que le code de sécurité a été généré ou le processus arrive à expiration.

Avertissement Vous devez conserver le code de sécurité dans un endroit sûr. S'il est nécessaire de régénérer ou de réinitialiser le token, ceci est impossible sans le code de sécurité.

Ne stockez pas le code de sécurité sur le token 3SKey NG-FLASH lui-même, ou avec votre token.

Si vous stockez le code de sécurité sur votre PC et que vous changez de PC, vous devez supprimer le code de sécurité de l'ancien PC et le stocker sur le nouveau.

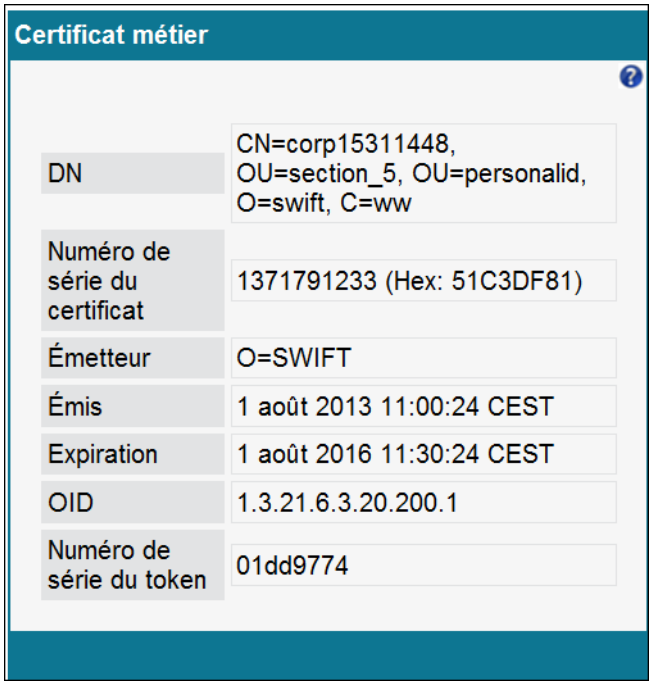
Seul le code de sécurité le plus récent est valide. Si un nouveau code de sécurité est généré pour un token, l'ancien code de sécurité deviendra invalide.

16 Informations portées par la clé - détails du certificat et du token

Présentation

La page **Informations portées par la clé** affiche des informations détaillées sur le token avec lequel vous êtes connecté et le certificat qu'il contient.

Écran



Champs

DN

Nom distinctif du certificat du token.

Le champ **CN** du nom distinctif contient l'identifiant unique du certificat.

Remarque Même si le numéro de série du certificat change, l'identifiant unique d'un certificat métier d'entreprise est préservé s'il est nécessaire de renouveler le certificat, de le régénérer sur un autre token ou de réinitialiser un token.

Numéro de série du certificat

Numéro de série du certificat, au format décimal et hexadécimal.

Émetteur

Émetteur du token. Il s'agit toujours de SWIFT.

Émis

Date et heure d'émission du certificat.

Expiration

Date et heure d'expiration du certificat.

OID

Identifiant d'objet du certificat du token.

Numéro de série du token

Numéro de série du fabricant imprimé sur le token.

17 Glossaire

Activer

Le token fourni par SWIFT contient initialement un certificat technique qui ne peut pas être utilisé pour signer des messages commerciaux. Le processus de conversion du certificat technique sur le token en un certificat métier est appelé **activation du token**. Pour des informations complémentaires, reportez-vous à "Activer un token", page 27.

Alias

Un administrateur 3SKey peut attribuer un **Alias** à un token, pour spécifier un nom avec lequel identifier le propriétaire du token. Par exemple, l'alias peut spécifier le nom ou le rôle de l'opérateur auquel il a été attribué, ou peut simplement être un libellé tel que **Token de réserve**.

L'alias est utilisé pour faciliter la gestion des tokens anonymes sur le portail 3SKey. Il n'a aucune incidence sur le portail de signature, et il n'est pas connu de la banque.

L'alias peut contenir les caractères suivants:

`A-Z`

`a-z`

`0-9`

`_ - ,` et espace

Vous ne pouvez pas utiliser de caractères accentués (é ou ö par exemple), ni de signes de ponctuation exceptés ceux qui sont répertoriés.

Certificat métier

Le processus d'activation 3SKey remplace le certificat technique du token par le certificat métier. Le certificat métier est utilisé pour sécuriser toutes les transactions commerciales avec les banques.

Le certificat métier est valide pendant trois ans à partir de la date d'activation.

Certificat technique

Le certificat technique est le certificat initial stocké par SWIFT sur un token non activé qui garantit que le token a été personnalisé par SWIFT. Il fournit une piste d'audit incontestable pour la création du certificat métier associé.

Le certificat technique n'est pas accepté pour l'authentification de transactions commerciales. Le token doit d'abord être activé pour produire un certificat métier.

Le certificat technique est valide pendant cinq ans. Après l'activation, le certificat métier est valide pendant trois ans.

Code de sécurité

Le code de sécurité est généré au cours du processus d'activation du token.

Il est utilisé pour:

- révoquer un token perdu ou compromis
- réinitialiser un token verrouillé ou dont le mot de passe est perdu
- régénérer l'identifiant unique sur un nouveau token

Le code de sécurité est téléchargé dans un fichier. Par défaut, le nom du fichier est **code.txt**.

Vous devez conserver le code de sécurité dans un endroit sûr mais accessible. Ne stockez pas le code de sécurité sur le token 3SKey NG-FLASH lui-même, ou avec votre token.

Si vous stockez le code de sécurité sur votre PC et que vous changez de PC, n'oubliez pas de supprimer le code de sécurité de l'ancien PC et stockez-le sur le nouveau.

Groupe d'utilisateurs

Le groupe d'utilisateurs est un ensemble de tokens 3SKey au sein d'une organisation spécifique. Le groupe d'utilisateurs est une aide pour gérer les tokens de l'organisation: il n'a aucun impact sur la capacité du token à signer des transactions, car l'application de signature ne connaît pas le groupe auquel le token appartient.

Un groupe d'utilisateurs peut contenir tous les tokens 3SKey appartenant à une organisation. Une organisation peut également avoir plusieurs groupes d'utilisateurs, généralement regroupés selon le lieu ou le service dans lequel les tokens sont utilisés.

Le système permet de créer un groupe d'utilisateurs à chaque fois qu'un utilisateur se connecte avec un token qui n'appartient pas encore à un groupe d'utilisateurs. Pour ajouter un token à un groupe d'utilisateurs existant, connectez-vous avec l'un des 2 tokens administrateur de ce groupe.

Pour des informations complémentaires, reportez-vous à "Gérer un groupe d'utilisateurs (pour les administrateurs)", page 21.

Identifiant unique

SWIFT crée un identifiant unique pour chaque token et le stocke dans le certificat technique sur le token non activé.

Lorsque le token est activé, l'identifiant unique est transféré sur le certificat métier. L'identifiant unique doit ensuite être enregistré auprès de la banque associée pour identifier un utilisateur spécifique comme propriétaire d'un identifiant unique spécifique.

L'identifiant unique est préservé durant le processus de renouvellement étant donné que le certificat sur le nouveau token aura le même identifiant unique que le certificat précédent sur l'ancien token.

Si le token est perdu ou compromis, il est possible de régénérer l'identifiant unique en le transférant sur un autre token. Pour des informations complémentaires, reportez-vous à "Régénérer un token", page 70.

Mot de passe

Chaque token comporte un mot de passe qui protège l'accès au token. Vous devez modifier le mot de passe pendant le processus d'activation.

Vous pouvez le modifier à nouveau en vous connectant au portail 3SKey et en utilisant la fonction **Modifier le mot de passe**.

Fournissez un mot de passe sécurisé. Suivez les directives ci-après lorsque vous créez un mot de passe:

- La longueur minimale est de quatre caractères
- La longueur maximale est de seize caractères
- Vous pouvez utiliser les caractères suivants:
  - `0-9 A-Z a-z` et espace
  - `_ ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~`

- Vous devez utiliser au moins deux caractères différents. Par exemple, vous ne pouvez pas définir le mot de passe sur `aaaa` ou `11111`
- Vous ne pouvez pas utiliser de caractères accentués (é ou ö par exemple)
- Vous ne pouvez pas réutiliser le mot de passe actuel ni le mot de passe précédent

Important Le mot de passe n'expire pas, mais SWIFT recommande de le modifier tous les trois mois.

Nom distinctif

Le nom distinctif (DN) est l'identification du certificat en suivant la notation X.500. Il se présente sous la forme `cn=corp<nnnnnnnn>, ou=section_n, ou=personalid, o=swift, c=ww`.

L'élément `cn` du nom distinctif est l'identifiant unique du token.

Régénération

Vous pouvez utiliser le processus de régénération si un token a été perdu, endommagé, si le certificat a été révoqué ou a expiré, ou encore si un token se trouve en période de renouvellement (90 jours avant expiration) et se verrouille.

Le processus de régénération vous permet de réutiliser l'identifiant unique de l'ancien token, et de l'associer à un autre token.

Pour des informations complémentaires, reportez-vous à "Régénérer un token", page 70.

Réinitialisation

Les utilisateurs d'entreprise peuvent réinitialiser leur token dont le mot de passe est perdu ou lorsque le token est verrouillé après saisie de 5 mots de passe incorrects. Le processus de réinitialisation permet aux utilisateurs de ré-initialiser leur token avec leur identifiant unique.

Pour des informations complémentaires, reportez-vous à "Réinitialiser un token dont le statut est Activated (Activé)", page 49.

Renouvellement

Les tokens 3SKey comprennent un certificat métier qui reste valide 3 ans à partir de la date d'activation du token. Par exemple, un token activé le 1er janvier 2011 comprend un certificat qui expire le 1er janvier 2014.

SWIFT recommande aux utilisateurs de renouveler les certificats sur un nouveau token au moins 2 mois avant la date d'expiration du certificat.

Pour des informations complémentaires, reportez-vous à "Renouveler un token", page 35.

Révocation

La révocation d'un token est nécessaire si vous avez perdu le token, ou si vous suspectez qu'il a été compromis. La révocation du token rend non valides tous les certificats associés à votre identifiant unique.

Vous pouvez régénérer l'identifiant unique d'un token révoqué sur un nouveau token, mais le token révoqué lui-même ne peut plus être utilisé.

Pour des informations complémentaires, reportez-vous à "Révoquer un token", page 63.

Rôles

Les rôles déterminent les fonctions qu'un utilisateur du service 3SKey peut effectuer sur le portail 3SKey. La plupart des utilisateurs ont le rôle `user`, mais il y a également des administrateurs qui ont le rôle `admin`.

Les utilisateurs avec le rôle `user` ont accès aux fonctions suivantes:

- Utiliser le certificat sur le token pour authentifier ou signer des transactions avec une banque
- Modifier le mot de passe du token
- Générer un nouveau code de sécurité
- Révoquer le certificat sur le token
- Effectuer la régénération du certificat sur un token. Pour cela, un second token préparé par un administrateur en vue d'une régénération est nécessaire.
- Effectuer la réinitialisation du token. Pour cela, un administrateur doit avoir préparé le token en vue d'une réinitialisation.
- Afficher les informations portées par la clé stockées sur le token (par exemple, l'identifiant unique et la période de validité)
- Renouveler le certificat sur un nouveau token avant son expiration (au bout de trois ans)

Les utilisateurs avec le rôle `admin` ont accès à toutes les fonctions du rôle `user`, plus les fonctions suivantes:

- Configurer et maintenir un groupe d'utilisateurs contenant des tokens avec le rôle `admin` et des tokens avec le rôle `user`
- Afficher les tokens et le statut des tokens dans le groupe d'utilisateurs
- Révoquer les tokens des utilisateurs dans le groupe
- Configurer un token pour la régénération d'un identifiant unique (rôle `user` ou rôle `admin`)
- Réinitialiser un token dont le statut est **NotActivated** (Non activé)
- Configurer en vue d'une réinitialisation un token dont le statut est **Activated** (Activé) qui est verrouillé ou dont le mot de passe est perdu

Utilisateur

Un utilisateur 3SKey est une personne individuelle associée à un identifiant unique. L'identifiant unique se trouve dans le DN du certificat stocké sur un token spécifique que l'utilisateur utilise pour signer des transactions avec une ou plusieurs banques.

18 Conditions générales

Bienvenue sur le portail 3SKey

La fourniture et l'utilisation du service 3SKey sont régies par les Conditions générales de 3SKey. Seule fait foi la dernière version en anglais disponible sur www.swift.com > À propos de SWIFT > Informations légales > Contrats SWIFT.

Pour plus d'informations sur les fonctionnalités et les fonctions de la solution 3SKey, et sur vos rôles et responsabilités en tant qu'utilisateur 3SKey ou abonné 3SKey ou sur ceux de SWIFT en tant que fournisseur de la solution 3SKey, consultez régulièrement la dernière version disponible de la Description du service 3SKey sur www.swift.com > Assistance > Documentation.

Important La fourniture et l'utilisation des tokens 3SKey sont soumises aux restrictions d'exportation des États-Unis et autres programmes de sanction. **Les personnes situées à ou originaires de Cuba, de Corée du Nord, d'Iran, du Soudan, de Libye ou de Syrie et les personnes identifiées sur des listes du gouvernement des États-Unis ou de l'Union européenne comme "partie refusée", ou sur des listes nationales désignées spécifiquement, ne sont pas autorisées à posséder ni à utiliser des tokens 3SKey**.

19 Assistance 3SKey

Assistance pour les clients 3SKey

Cette section décrit les types d'assistance fournis par SWIFT aux utilisateurs 3SKey.

SWIFT est l'unique point de contact pour reporter tous les problèmes et requêtes relatifs à l'installation des tokens 3SKey, à l'activation et à la gestion sur le portail 3SKey.

Pour toute autre question, les clients d'entreprises sont priés de contacter leur banque.

Procédez par étapes pour résoudre votre problème:

1. Consultez le Guide de dépannage 3SKey.

   Si le problème n'est pas résolu, passez à l'étape suivante.

2. Consultez l'auto-assistance sur le portail.

   Pour accéder à l'auto-assistance 3SKey, accédez à **www.3skey.com**, cliquez sur **Aide**.

   La liste des sujets traités dans **l'auto-assistance 3SKey** s'affiche.

   Si le problème n'est pas résolu, passez à l'étape suivante.

3. Consultez le tableau ci-dessous pour identifier le point de contact le plus approprié.

Type de problème	Contact = SWIFT	Contact = votre banque
Enregistrement du token activé		X
Mot de passe d'activation pour les nouveaux tokens		X
Installation du logiciel du token	X	
Connexion au portail 3SKey	X	
Gestion du token sur le portail 3SKey(1)	X	
Commande de tokens		X
Mot de passe après activation	X	
Transactions rejetées		X
Application de signature / trésorerie (configuration des certificats)		X (ou application de signature / trésorerie)
Application de signature / trésorerie (problèmes généraux)	X (si la connexion au portail 3SKey est impossible)	X (si la connexion au portail 3SKey fonctionne, veuillez contacter votre banque ou le vendeur de l'application de signature / trésorerie)

(1) La gestion des tokens comprend la création de groupes d'utilisateurs, la gestion des groupes d'utilisateurs, l'activation, la modification du mot de passe, la génération du code de sécurité, l'ajout d'utilisateurs, la régénération, la réinitialisation, le renouvellement et la révocation.

Si le point de contact le plus approprié est une entité autre que SWIFT, veuillez contacter cette entité.

Si le point de contact le plus approprié est SWIFT, passez à l'étape suivante.

4. Contactez l'assistance 3SKey par e-mail (reportez-vous à la section **Assistance par e-mail** ci-dessous).

   Si le problème n'est pas résolu, passez à l'étape suivante.

5. Contactez un analyste du service d'assistance (reportez-vous à la section **Assistance téléphonique** ci-dessous).

Assistance par e-mail

Si vous n'avez pas été en mesure de résoudre votre problème à l'aide du Guide de dépannage 3SKey ou de l'auto-assistance 3SKey, envoyez un e-mail à 3skey.support@swift.com.

Veuillez inclure les informations suivantes dans le message électronique. Un analyste du service d'assistance étudiera votre problème et vous contactera.

Remarque L'analyste vous fournira un numéro de dossier qui servira de référence si vous devez contacter l'assistance téléphonique.

1. Coordonnées
   - Prénom et nom
   - Adresse e-mail
   - Numéro de téléphone
   - Numéro de téléphone mobile
   - Nom de l'entreprise
   - Description claire du problème
   - Numéro de série indiqué sur le token
2. Quelle opération effectuez-vous sur le portail 3SKey?
   - Installation du logiciel du token
   - Création d'un groupe d'utilisateurs
   - Connexion
   - Activation
   - Régénération
   - Révocation
   - Réinitialisation
   - Renouvellement
3. Quel message d'erreur avez-vous reçu?
4. Quel est votre rôle sur 3SKey et êtes-vous le propriétaire du token?

Important Veuillez zipper et joindre les fichiers journaux d'installation à l'e-mail.

Voici les différents emplacements par défaut où sont disponibles les fichiers journaux en fonction de la version du programme d'installation que vous utilisez:

- 3SKey_token_install.exe (mars 2013)
  - **C:\Program Files\Swift\Swift Token Client\logs** (système 32 bits)
  - **C:\Program Files (x86)\Swift\Swift Token Client\logs** (système 64 bits)
- SwiftTokenClient-2.0x64wrapper.exe ou SwiftTokenClient-2.0x32wrapper.exe (février 2012)
  - **C:\Program Files\Swift\Swift Token Client 2.0\logs**
- 3SKeyinstall.exe (avant février 2012)
  - **C:\Program Files\3SKey\logs**

Si vous n'avez pas encore installé le logiciel 3SKey, veuillez fournir les détails de votre système d'exploitation. Ces détails comprennent la version et le service pack de Windows, la version d'Internet Explorer ainsi que la version de Java que vous utilisez.

Assistance téléphonique

Si votre question n'a pu être résolue par les moyens décrits ci-avant, vous pouvez contacter un analyste du service d'assistance par téléphone. Nos analystes du service d'assistance sont disponibles pour vous aider pendant les heures de bureau, du lundi au vendredi.

Asie-Pacifique:	**+33-1 57 32 35 36** de 09h00 à 12h00 et de 14h00 à 17h00 CET (GMT+2)
Europe, Moyen-Orient et Afrique:	**+33-1 57 32 35 36** de 09h00 à 12h00 et de 14h00 à 17h00 CET (GMT+2)
Amériques:	**+1-540 727 1685** de 09h00 à 18h00 EST (GMT-4)

Mentions légales

Copyright

SWIFT © 2015. Tous droits réservés.

Clause de protection

Les informations contenues dans cette publication sont susceptibles d'être modifiées ponctuellement. Vous devez toujours vous reporter à la dernière version disponible.

Traductions

La version anglaise de la documentation SWIFT est la seule version officielle et contraignante.

Marques commerciales

SWIFT est le nom commercial de S.W.I.F.T. SCRL. Les noms suivants sont des marques déposées de SWIFT: le logo SWIFT, SWIFT, SWIFTNet, Accord, Sibos, 3SKey, Innotribe, le logo Standards Forum, MyStandards, et SWIFT Institute. Les autres noms de produit, de service ou d'entreprise dans cette publication sont des noms commerciaux, des marques commerciales ou des marques déposées de leurs propriétaires respectifs.